UTILITAS MATHEMATICA 128 (2026) 329–373

Utilitas Mathematica
www.combinatorialpress.com/um

Combinatorial Press

Solutions of equations $ax^m + by^m - cz^m = 1$ over finite fields

Wen-Fong Ke and Hubert Kiechle*

ABSTRACT

We investigate diagonal equations $ax^m + by^m - cz^m = 1$ over finite fields F using combinatorial designs naturally associated with F. Building on prior work that resolved the case $a = b = c = 1$, we obtain exact formulas for the solutions when $a = 1$ and $b = c$, under circularity assumptions. For general coefficients, we present an algorithm that determines whether a given instance can be reduced to the settled cases, or else identifies it as requiring brute-force computation.

Keywords: diagonal equation, Ferrero pair, circular Ferrero pair, 2-design, circular 2-design, overlap graphs

2020 Mathematics Subject Classification: 11D41, 11T23.

1. Introduction

Let F be a finite field of characteristic p. For fixed $a, b, c \in F^*$ and a positive integer m, we consider the diagonal equation

$$ax^m + by^m - cz^m = 1, \tag{1}$$

and aim to determine its number of solutions N in F, under assumptions to be specified later. Our method is to study intersection patterns among certain subsets of F. For the case $a = 1$ and $b = c$, we obtain decisive results. While a complete analysis is not feasible for arbitrary a, b, c, we offer an algorithm that provides a framework which may succeed in computing N, or at least narrowing the possibilities. Examples will be provided to illustrate its behavior.

* Corresponding author.

Received 16 Apr 2026; Revised 03 Jul 2026; Accepted 09 Jul 2026; Published Online 22 Jul 2026.

DOI: 10.61091/um128-17

Well-known formulas for the number of solutions to Eq. (1) involving Jacobi sums (see [7, Ch. 8 Thm. 5] for a comprehensive exposition and [8] for further references). These formulas are difficult to evaluate and are primarily used to derive the classical estimates of Hua and Vandiver [5], as well as Weil [19].

Suppose that F has q elements; thus, q is a power of a prime p. Since N remains unchanged when m is replaced by $\gcd(m, q-1)$ (cf. [8]), we may assume without loss of generality that $m \mid (q-1)$ and $1 < m < q-1$. We define $k = (q-1)/m$.

Simple formulas for N are known only in special cases—particularly when m is small ([3, 14]), when k is small ([14]), or when q is a square ([4, 6, 20]).

Let Φ denote the subgroup of the multiplicative group $F^* = F \setminus \{0\}$ of order k. We refer to the pair (F, Φ) as a *Ferrero pair*. Although the standard definition of a Ferrero pair is more eneral (see [1]), the present formulation suits our purposes. Note that the parameters (q, k) uniquely determine (F, Φ). As shorthand, we will refer to (F, Φ) simply by (q, k), and also call (q, k) a *Ferrero pair*.

Throughout, we impose a geometrical condition on (F, Φ) (or (q, k)) called "circularity". We say that (F, Φ) (and (q, k)) is *circular* when

$$|\Phi r \cap (\Phi u + v)| \leq 2 \quad \text{for all } r, u, v \in F^*,$$

where $\Phi r = \{\phi r \mid \phi \in \Phi\}$ $(= r\Phi)$ and $\Phi u + v = \{\phi u + v \mid \phi \in \Phi\}$. These are referred to as "Φ-blocks". For many results, we will also impose slightly stronger conditions involving intersections of certain Φ-blocks, which are closely related to cyclotomic numbers. These aspects will be addressed in Section 2.

Contrary to the tradition in algebraic geometry, we keep k fixed rather than m. Consequently, in the circular case, m is always a large divisor of $q-1$ (see [12, 13]).

Estimates derived from Hua-Vandiver or Weil's theorems assume q to be sufficiently large. Our results apply in situations where these classical estimates fail, as discussed in detail in [9].

As mentioned above, we have decisive results on the number of solutions for the equation

$$x^m + by^m - bz^m = 1, \tag{2}$$

where $b \in F^*$. We now give an overview of these results. Let N_b denote the number of solutions to (2). First, we note the trivial identity $N_b = N_{-b}$.

We begin with the base case $b = c = 1$. This case was first considered in [9] and then updated in [12]. Note that the condition $b \in \Phi$, rather than $b = 1$, does not make any difference.

Theorem 1.1 ([12, Theorem 1]). *Let (F, Φ) be circular and assume $b \in \Phi$. Let N_b be the number of solutions of the equation $x^m + by^m - bz^m = 1$.*

(1) *If k is even, then*

$$N_b = N_{-b} = \begin{cases} 3(k-1)m^3 + 6m^2 + 3m & \text{if } 6 \mid k, \\ 3(k-1)m^3 + 3m^2 + 3m & \text{if } p = 3, \\ 3(k-1)m^3 + 3m & \text{otherwise.} \end{cases}$$

(2) *If k is odd, then*

$$N_b = N_{-b} = \begin{cases} (3k-2)m^3 + 6m^2 + 3m & \text{if } p = 2 \text{ and } 3 \mid k, \\ (3k-2)m^3 + 3m & \text{if } p = 2 \text{ and } 3 \nmid k, \\ (2k-1)m^3 + 3m^2 + 2m & \text{if } 2 \in \Phi, \\ (2k-1)m^3 + 2m & \text{otherwise.} \end{cases}$$

Throughout the paper, we shall fix a generator φ of the cyclic group Φ and define

$$c_{j,i} = (\varphi^j - 1)^{-1}(\varphi^i - 1) \quad \text{for } i, j \in \boldsymbol{k} = \{1, 2, \ldots, k-1\}.$$

Also, denote by $\mathcal{D}$ the union of all such cosets $\Phi c_{j,i}$ of Φ in F^*. Thus,

$$\mathcal{D} = \cup_{i,j \in \boldsymbol{k}} \Phi c_{j,i} = \{\lambda c_{j,i} \mid \lambda \in \Phi,\ i, j \in \boldsymbol{k}\}.$$

For the moment, it suffices to say that in order for the equation $x^m + by^m - bz^m = 1$ to have solutions $x, y, z \in F^*$ with $y^m \neq z^m$, the element b must lie in a coset $\Phi c_{j,i}$ for some i, j, or equivalently $b \in \mathcal{D}$.

Let us consider first the case when k is even. The following theorem, a direct consequence of (22), Theorems 3.3, 3.14 and Lemma 4.1 (whose proofs are deferred), settles the situation when b avoids exceptional cosets. Specifically, these cosets are

$$\Phi(\varphi^{\frac{k}{2}} - 1) = 2\Phi, \quad \Phi(\varphi^{\frac{k}{2}} - 1)^{-1} = 2^{-1}\Phi.$$

Note that Lemma 4.1 shows that whenever $6 \mid k$, we always have $b \notin 2\Phi \cup 2^{-1}\Phi$. Further phenomena, tied to divisibility conditions on k, will be addressed in subsequent sections.

Theorem 1.2. *Let (F, Φ) be circular with k even, and $b \in F^* \setminus \mathcal{D}$. If $b \notin 2\Phi \cup 2^{-1}\Phi$, then $N_b = km^3 + m$.*

After settling the case when $b \notin \mathcal{D} \cup 2\Phi \cup 2^{-1}\Phi$, the complementary situation arises: either b is in some cosets $\Phi c_{j,i}$ with $i \neq j$ or in the exceptional sets $2\Phi \cup 2^{-1}\Phi$. For the case $6 \mid k$, we summarize the outcomes in a table (Table 1), accompanied by two theorems (Theorems 1.3 and 1.4). Finally, Theorem 1.5 completes the analysis by handling the remaining even-k cases when $3 \nmid k$. Taken together, these results provide a complete description of the values of N_b when k is even.

To organize the analysis, we introduce the sets A and A^{-1}. Define

$$A = \{\psi(\lambda - 1) \mid \psi, \lambda \in \Phi,\ \lambda \neq 1\} = \cup_{\chi \in \Phi, \chi \neq 1} \Phi(\chi - 1), \tag{3}$$

and set

$$A^{-1} = \{u^{-1} \mid u \in A\}.$$

Since Φ is a group, it follows that

$$A^{-1} = \{\psi(\lambda - 1)^{-1} \mid \psi, \lambda \in \Phi,\ \lambda \neq 1\} = \cup_{\chi \in \Phi, \chi \neq 1} \Phi(\chi - 1)^{-1}.$$

Furthermore, it follows from Lemma 2.8 ([12, Lemma 9]) that when k is even or $p = 2$, the cosets $\Phi(\varphi^i - 1) = \Phi(\varphi^j - 1)$, $i, j \in \boldsymbol{k}$, only if $i = j$ of $i = k - j$, and when k is odd and $p \neq 2$, all cosets $\Phi(\varphi^i - 1)$, $i \in \boldsymbol{k}$, are distinct.

In Table 1, Special configurations, including all cases with b in $A \cap A^{-1}$ as well as certain additional situations, are recorded; each row specifies the corresponding value of N_b and cites the theorem where the proof appears (see Section 5). In analyzing these cases we rely on the notion of overlaps introduced in [11], together with the classification theorem ([11, Theorem 5.1]) presented in Subsections 2.2 and 2.3.

Table 1. Special cases assuming $6 \mid k$, $p \notin \mathcal{Q}_k$, and $b \in A \cup A^{-1}$

	Condition of b	Numbers	Theorem
	$b \in \Phi = \Phi(\varphi^{\frac{k}{6}} - 1)$	$N_b = 3(k-1)m^3 + 6m^2 + 3m$	1.1, §5
	$b \in 2\Phi = \Phi(\varphi^{\frac{k}{2}} - 1)$	$N_b = (k+2)m^3 + 2m^2 + m$	5.1(2)
	$b \in 2^{-1}\Phi = \Phi(\varphi^{\frac{k}{2}} - 1)^{-1}$	$N_b = (k+2)m^3 + m^2 + m$	
	$b \in \Phi(\varphi^{\frac{k}{3}} - 1)$	$N_b = (k+4)m^3 + 4m^2 + m$	5.2
	$b \in \Phi(\varphi^{\frac{k}{3}} - 1)^{-1}$	$N_b = (k+4)m^3 + 2m^2 + m$	
$12 \mid k$	$b \in \Phi(\varphi^{\frac{k}{4}} - 1)$	$N_b = (k+6)m^3 + 4m^2 + m$	5.3
	$b \in \Phi(\varphi^{\frac{k}{4}} - 1)^{-1}$	$N_b = (k+6)m^3 + 2m^2 + m$	
	$b \in \Phi(\varphi^{\frac{k}{12}} - 1) \cup \Phi(\varphi^{\frac{5k}{12}} - 1)$	$N_b = (k+8)m^3 + 6m^2 + m$	5.4
$30 \mid k$	$b \in \Phi(\varphi^{\frac{k}{10}} - 1) \cup \Phi(\varphi^{\frac{3k}{10}} - 1)$	$N_b = (k+12)m^3 + 6m^2 + m$	5.5
	$b \in \Phi(\varphi^{\frac{k}{15}} - 1) \cup \Phi(\varphi^{\frac{2k}{15}} - 1) \cup$		
	$\cup\, \Phi(\varphi^{\frac{4k}{15}} - 1) \cup \Phi(\varphi^{\frac{7k}{15}} - 1)$	$N_b = (k+12)m^3 + 4m^2 + m$	5.6
	$b \in \Phi(\varphi^{\frac{k}{15}} - 1)^{-1} \cup \Phi(\varphi^{\frac{2k}{15}} - 1)^{-1} \cup$		
	$\cup\, \Phi(\varphi^{\frac{4k}{15}} - 1)^{-1} \cup \Phi(\varphi^{\frac{7k}{15}} - 1)^{-1}$	$N_b = (k+12)m^3 + 2m^2 + m$	5.6

The first of the two theorems, Theorem 1.3, covers those b in $A \cup A^{-1}$ that do not satisfy any of the conditions listed in Table 1. The proof will be given at the end of Section 5.1 after Theorem 5.6. The set $\mathcal{Q}_k$ in the statement is a finite set consisting of "exceptional" primes, to be described in Theorem 2.10.

Theorem 1.3. *Let (F, Φ) be a Ferrero pair with $p \notin \mathcal{Q}_k$ and $6 \mid k$. If $b \in A \cup A^{-1}$ and b does not match any of the conditions displayed in Table 1. Then*

$$N_b = \begin{cases} (k+8)m^3 + 4m^2 + m & \text{if } b \in A \setminus A^{-1}, \\ (k+8)m^3 + 2m^2 + m & \text{if } b \in A^{-1} \setminus A. \end{cases}$$

The second theorem, Theorem 1.4, addresses the complementary case $b \notin A \cup A^{-1}$. It distinguishes between situations where b is or is not involved in a nontrivial overlap. If b is not involved in any overlap, the formulas for N_b apply without further restriction. By contrast, to have b involved in a nontrivial overlap requires $6 \mid k$. The theorem will be proved in Section 5.2.

Theorem 1.4. *Let (F, Φ) be a Ferrero pair with $p \notin \mathcal{Q}_k$ and k even. If $b \in \Phi c_{i,j}$ with $b \notin A \cup A^{-1}$, then the following cases can occur:*

$$N_b = \begin{cases} (k+2)m^3 + m & \text{if } i = \frac{k}{2} \text{ or } j = \frac{k}{2}, \\ (k+4)m^3 + m & \text{if } \frac{k}{2} \notin \{i, j\}, \text{ and } c_{j,i} \text{ is not involved in a nontrivial overlap}, \\ (k+8)m^3 + m & \text{if } \frac{k}{2} \notin \{i, j\}, \text{ and } c_{j,i} \text{ is involved in a nontrivial overlap}. \end{cases}$$

The following theorem, Theorem 1.5, handles the cases when $3 \nmid k$ and completes the enumerations for even k. Its formula for N_b arises by combining the cubic term from Theorems 3.5 with the quadratic coefficient α introduced in Section 3. The precise determination of α will be given in Section 3.2, specifically, in Theorem 3.13, but the general form of the result can already be stated here.

Theorem 1.5. *Let (F, Φ) be a Ferrero pair with $p \notin \mathcal{Q}_k$ with even k and $3 \nmid k$. If $b \in \Phi c_{i,j}$ for some distinct $i, j \in \{1, 2, \ldots, k-1\}$, then*

$$N_b = \begin{cases} (k+2)m^3 + \alpha m^2 + m & \text{if } i = \frac{k}{2} \text{ or } j = \frac{k}{2}, \\ (k+4)m^3 + \alpha m^2 + m & \text{otherwise}. \end{cases}$$

Here $\alpha = 2t_b + t_{b^{-1}}$, as defined in Theorems 3.13 and 3.14.

Having settled the even-k cases through Table 1 and Theorems 1.2–1.5, now turn to the situation when k is odd, and pack them in two theorems. In this regime, besides excluding the finite set of exceptional primes Q_k, we must also exclude the primes from the finite set $\mathcal{A}_k$ defined in Lemma 4.12. These theorems will be established once Theorem 3.3, Theorem 3.4, Lemma 3.7 and Corollary 4.17 are proved in Sections 3 and 4. Since their proofs follow directly from those results, we record their statements here for completeness but omit separate proofs.

We begin with the case $b \notin \mathcal{D}$. In this situation, one cannot have $-b \in \Phi$: for if $b = -\varphi^s$ for some $s \in \{0, 1, 2, \ldots, k\}$, then $b = -\varphi^s = \frac{\varphi^s - 1}{\varphi^{k-s} - 1}$, which forces $b \in \mathcal{D}$, a contradiction. Hence whenever $b \notin \mathcal{D}$, it follows automatically that $-b \notin \Phi$. In the enumeration formula, the factors of m^3 are determined using Theorem 3.3(1), those of m^2 from Corollary 4.17, and that of m comes from Lemma 3.7. This yields the following result.

Theorem 1.6. *Let (F, Φ) be a Ferrero pair with k odd and $p \notin \mathcal{Q}_k \cup \mathcal{A}_k$. Suppose that $b \in F^* \setminus \mathcal{D}$. Then $-b \notin \Phi$, and*

$$N_b = \begin{cases} km^3 + 2m^2 + m & \text{if } b \in A, \\ km^3 + m^2 + m & \text{if } b \in A^{-1}, \\ km^3 + m & \text{if } b \notin A \cup A^{-1}. \end{cases}$$

We now turn to the situation when b is in $\mathcal{D}$. Unlike the previous case, here the condition $-b \in \Phi$ may or may not hold, so both possibilities must be considered. In the enumeration formula, the factors of m^3 are determined using Theorem 3.4, while the factors of m^2 and m come from the same sources as before—Corollary 4.17 and Lemma 3.7, respectively. The precise contributions depend on whether $-b$ lies in Φ and on the value of p. This leads to the following result:

Theorem 1.7. *Let (F,Φ) be a Ferrero pair with k odd and $p \notin \mathcal{Q}_k \cup \mathcal{A}_k$. Suppose that $b \in \mathcal{D} \setminus \Phi$.*

(1) *If $p \neq 2$ and $-b \notin \Phi$, then*

$$N_b = \begin{cases} (k+2)m^3 + 2m^2 + m & \text{if } b \in A, \\ (k+2)m^3 + m^2 + m & \text{if } b \in A^{-1}, \\ (k+2)m^3 + m & \text{if } b \notin A \cup A^{-1}. \end{cases}$$

(2) *If $p \neq 2$ and $-b \in \Phi$, then*

$$N_b = \begin{cases} (k+2)m^3 + 2m^2 + 2m & \text{if } b \in A, \\ (k+2)m^3 + m^2 + 2m & \text{if } b \in A^{-1}, \\ (k+2)m^3 + 2m & \text{if } b \notin A \cup A^{-1}. \end{cases}$$

(3) *If $p = 2$, then*

$$N_b = \begin{cases} (k+4)m^3 + 2m^2 + m & \text{if } b \in A, \\ (k+4)m^3 + m^2 + m & \text{if } b \in A^{-1}, \\ (k+4)m^3 + m & \text{if } b \notin A \cup A^{-1}. \end{cases}$$

Together, Theorems 1.6 and 1.7 exhaust all possibilities when k is odd, completing the enumerations of N_b in this setting. The condition in Theorem 1.7 can be strengthened by enlarging the excluded set of primes to $\mathcal{Q}_k \cup \mathcal{A}_k \cup \mathcal{B}_k$, where $\mathcal{B}_k$ is another finite set. Under this stronger assumption one has $A \cap \mathcal{D} = \varnothing$, and the classification of N_b for odd k becomes more compact. Since these sets are finite, this refinement only affects finitely many primes. For clarity of presentation, we do not pursue this direction further, as the classification above already covers all odd-k cases.

2. Preliminaries

In this section, we develop the geometric framework that underpins our method. We begin by establishing a link between the solutions to the equation

$$ax^m + by^m - cz^m = 1,$$

over F and the intersection patterns among certain Φ-blocks of F. This connection motivates the graph-theoretic perspective introduced next, where basic results on intersection numbers of selected Φ-blocks are collected. We then present the classification of overlaps, including notation and results adapted from [11], which will be essential for the enumeration of N in later sections. Note that circularity is not assumed in Subsections 2.1 and 2.2 for (F,Φ) unless explicitly stated.

2.1. A link between solutions and intersections of Φ*-blocks*

Define

$$S = \{(x, y, z) \in F^3 \mid ax^m + by^m - cz^m = 1 \text{ with } xyz \neq 0\},$$
$$T = \{(x, y, z) \in F^3 \mid ax^m + by^m - cz^m = 1 \text{ with } xyz = 0\}.$$

Thus, the disjoint union $S \cup T$ is the complete set of solutions to the equation in F^3, while S consists of the solutions in $(F^*)^3$.

We can quickly relate $|S|$ to the total number of intersection points among certain Φ-blocks.

Suppose first that there exists

$$w \in (\Phi c + 1) \cap (\Phi b + \varphi^i a),$$

for some $i \in \boldsymbol{k}_0 = \{0, \ldots, k-1\}$. Then there are $s, t \in \boldsymbol{k}_0$ such that

$$\varphi^t c + 1 = w = \varphi^s b + \varphi^i a.$$

Let ζ be a generator F^* and put $\varphi = \zeta^m$. For arbitrary mth roots of unity $\lambda_1, \lambda_2, \lambda_3 \in \langle \zeta^k \rangle$, define

$$x = \lambda_1 \zeta^i, \quad y = \lambda_2 \zeta^s, \quad z = \lambda_3 \zeta^t,$$

and we have

$$ax^m + by^m - cz^m = a\lambda_1^m \zeta^{mi} + b\lambda_2^m \zeta^{ms} - c\lambda_3^m \zeta^{mt} = \varphi^i a + \varphi^s b - \varphi^t c = 1.$$

Therefore $(x, y, z) \in S$.

Conversely, let $(x, y, z) \in S$. Then $x = \zeta^{i'}$, $y = \zeta^{s'}$, and $z = \zeta^{t'}$ for some $i', s', t' \in \{1, 2, \ldots, q-1\}$. There exist integers i'', s'', t'' such that

$$i' = i''k + i, \quad s' = s''k + s, \quad t' = t''k + t,$$

with $i, s, t \in \boldsymbol{k}_0$. Then

$$x^m = \zeta^{i'm} = \varphi^i, \quad y^m = \zeta^{s'm} = \varphi^s, \quad z^m = \zeta^{t'm} = \varphi^t.$$

From $ax^m + by^m - cz^m = 1$, we obtain

$$1 + \varphi^t c = \varphi^s b + \varphi^i a \in (\Phi c + 1) \cap (\Phi b + \varphi^i a).$$

From these observations, it follows that

$$|S| = m^3 \cdot \sum_{i=0}^{k-1} |(\Phi c + 1) \cap (\Phi b + \varphi^i a)|. \tag{4}$$

Similarly, we can relate $|T|$ to the total number of intersection points among certain Φ-blocks. Define

$$T_x = \{(0, y, z) \in T \mid yz \neq 0\},$$

$$\begin{aligned}
T_y &= \{(x,0,z) \in T \mid xz \neq 0\},\\
T_z &= \{(x,y,0) \mid xy \neq 0\},\\
T_{x,y} &= \{(x,y,z) \in T \mid x = y = 0\},\\
T_{x,z} &= \{(x,y,z) \in T \mid x = z = 0\},\\
T_{y,z} &= \{(x,y,z) \in T \mid y = z = 0\}.
\end{aligned}$$

Then T is the disjoint union of T_x, T_y, T_z, $T_{x,y}$, $T_{x,z}$, and $T_{y,z}$. Using arguments similar to those for S, we find

$$\begin{aligned}
|T_x| &= m^2 \cdot |\Phi \cap (\Phi cb^{-1} + b^{-1})|,\\
|T_y| &= m^2 \cdot |\Phi \cap (\Phi ca^{-1} + a^{-1})|,\\
|T_z| &= m^2 \cdot |\Phi \cap (\Phi a + b)|.
\end{aligned} \tag{5}$$

Finally, the number of solutions to the equation $ex^m = 1$ in F (with $e \in F^*$) is m if $e \in \Phi$, and 0 otherwise. Thus, $|T_{x,y}|$ is either m or 0, depending on whether $-c \in \Phi$, and similarly for $|T_{x,z}|$ and $|T_{y,z}|$. See also Lemma 3.7.

In summary, the number of solutions to the equation $ax^m + by^m - cz^m = 1$ can be expressed explicitly in terms of the total number of intersection points among certain Φ-blocks, plus 0, m, $2m$, or $3m$, depending on whether a, b, and $-c$ lie in Φ. Theorem 1.1 is an example where (F, Φ) is circular and $a, b, c \in \Phi$, (in particular, for $a = 1$, and $b = c \in \Phi$).

2.2. *Some graphs on Φ-blocks and overlaps*

Let $r \in F$ be fixed, and let

$$E_r = \{\Phi + v \mid v \in \Phi r\}.$$

In [10], the intersection pattern for the Φ-blocks in E_r is illustrated using a graph. A colored graph $\Gamma_r = \Gamma(E_r) = (\mathcal{V}_r, \mathcal{E}_r)$ is associated to E_r as follows: the set $\mathcal{V}_r$ of vertices of Γ_r is simply the set Φ, and there is an n-edge $(\psi, \psi')_n$, with $1 \leq n < k$, connecting the vertices ψ and ψ' if

$$|(\Phi + \psi r) \cap (\Phi + \psi' r)| = n.$$

Note that, for all $\chi \in \Phi$,

$$|(\Phi + \psi r) \cap (\Phi + \psi' r)| = |(\Phi + \chi\psi r) \cap (\Phi + \chi\psi' r)|.$$

Suppose that Γ_r has an edge, i.e., $\mathcal{E}_r \neq \varnothing$. Then Φ acts on $\mathcal{E}_r$ via

$$\chi \bullet (\psi, \psi')_n = (\chi\psi, \chi\psi')_n \quad \text{for } \chi \in \Phi.$$

Then $\mathcal{E}_r$ is partitioned into a disjoint union of orbits, each containing edges of the same color and involving all vertices from Φ. Given an n-edge $(\psi, \psi')_n$, its orbit is denoted by $[(\psi, \psi')_n]$. If $\psi^{-1}\psi' = \varphi^j$, where $j \in \boldsymbol{k}$, then the n-edge $(1, \varphi^j)_n$ is in $[(\psi, \psi')_n]$, and so $[(\psi, \psi')_n] = [(1, \varphi^j)_n]$. In this case, the vertex set Φ together with the n-edges in $[(1, \varphi^j)_n]$ form a spanning subgraph of Γ_r, referred to as the jth *basic graph* in [10].

It is clear that if $[(1, \varphi^j)_n]$ and $[(1, \varphi^{j'})_{n'}]$ are nonempty, where $j, j' \in \boldsymbol{k}$, then they are disjoint orbits except when $j' = j$ or $j' = k - j$. When the edge set of Γ_r is the union of two or more such orbits, we say that an *overlap* occurs in Γ_r, and that r *is involved in an overlap*.

Now, let us collect some basic facts about the occurring of an edge and overlaps. Recall that

$$c_{j,i} = (\varphi^j - 1)^{-1}(\varphi^i - 1) \quad \text{for } i, j \in \boldsymbol{k},$$

and

$$\mathcal{D} = \{\lambda c_{j,i} \mid \lambda \in \Phi,\ i, j \in \boldsymbol{k}\} = \cup_{i,j \in \boldsymbol{k}} \Phi c_{j,i}.$$

It is immediate that $\Phi \subseteq \mathcal{D}$. Also for $i, j \in \boldsymbol{k}$ and $\lambda \in \Phi$, we have $(\lambda c_{j,i})^{-1} = \lambda^{-1} c_{i,j}$ and $-c_{j,i} = -(\varphi^j - 1)^{-1}(\varphi^i - 1) = (\varphi^j - 1)^{-1}(1 - \varphi^i) = \varphi^i(\varphi^j - 1)^{-1}(\varphi^{k-i} - 1) = \varphi^i c_{j,k-i}$.We record these easy observations here for later use.

Lemma 2.1. $\Phi \subseteq \mathcal{D} = \mathcal{D}^{-1} = -\mathcal{D}$.

According to [10, (4.3)], we have:

Lemma 2.2. *The graph Γ_r has an edge if and only if $r \in \mathcal{D}$.*

In fact, $(1, \varphi^j)_n$ is an edge of Γ_r exactly when $r \in \Phi c_{j,i}$ for some $i \in \boldsymbol{k}$. A more precise statement can be found in Lemma 3.2. From this, one immediately obtains:

Theorem 2.3. *An overlap occurs in Γ_r if and only if there exist $w \in \boldsymbol{k}_0$ and $i, j, s, t \in \boldsymbol{k}$ with $j \neq s$ such that*

$$c_{j,i} = (\varphi^j - 1)^{-1}(\varphi^i - 1) = \varphi^w(\varphi^s - 1)^{-1}(\varphi^t - 1) = \varphi^w c_{s,t}.$$

Remark 2.4. In Theorem 2.3, by taking $w = 0$, $j = i$, and $t = s$, one sees that the graph Γ_1 is in fact a complete graph. Thus, there is always an overlap with $\lfloor \frac{k}{2} \rfloor$ edges. This turns out to be the only overlap having $\lfloor \frac{k}{2} \rfloor$ edges. The number $\lfloor \frac{k}{2} \rfloor$ arises from the fact that $[(1, \varphi^j)_n] = [(1, \varphi^{k-j})_n]$ for all $j \in \boldsymbol{k}$, as we have seen above. For obvious reasons, we will later refer to these overlaps as trivial.

Recall that (F, Φ), or (q, k) (or even (p, k), to be explained next), is *circular* when

$$|\Phi r \cap (\Phi u + v)| \leq 2 \quad \text{for all } r, u, v \in F^*.$$

This is equivalent to the statement that any two distinct Φ-blocks intersect in at most two points—that is, they behave in a sense like circles. One important result from [15] is that circularity depends only on the characteristic of the field. Therefore, the phrase "(p, k) is circular" is justified.

The following results (1) and (2) can be found in [12]; (3) is an easy consequence.

Lemma 2.5 ([12, Lemma 10])**.** *Let (p, k) be circular. For $i, i', j \in \boldsymbol{k}$ we have*

(1) *If k is even, then* $c_{j,i} \in \Phi c_{j,i'} \iff i = i'$ *or* $i = k - i'$.

(2) *If k is odd, then* $c_{j,i} \in \Phi c_{j,i'} \iff i = i'$ *or, in case* $p = 2$, $i = k - i'$.

(3) *If k is odd and* $p \neq 2$, *then* $c_{j,i} \in -\Phi c_{j,i'} \iff i = k - i'$.

For $u, v \in F$ with $u \neq 0$, define

$$[u, v]_k = |\Phi \cap (\Phi u + v)|. \tag{6}$$

The symbol is closely related to cyclotomic numbers (cf. [16, Section 3.1]), as pointed out in detail in [12, Remark 17].

Lemma 2.6 ([12, Lemma 13]). *If* $u, v \in F^*$ *and* $\psi, \chi \in \Phi$, *then*

$$[u, v]_k = [\psi u, \chi v]_k = [v, u]_k = [-u^{-1}v, u^{-1}]_k.$$

From [12, Lemma 16, Lemma 19], we find:

Lemma 2.7. *Let (p, k) be circular and* $r \in F^*$

(1) *If k is even then*

$$[r, 1]_k = \begin{cases} 2 & \text{for } r \in \Phi(\psi - 1),\ \psi \in \Phi \setminus \{1, -1\}, \\ 1 & \text{for } r \in 2\Phi, \\ 0 & \text{otherwise.} \end{cases}$$

In particular,

$$[1, 1]_k = \begin{cases} 2 & \text{if } 6 \mid k, \\ 1 & \text{if } p = 3, \\ 0 & \text{otherwise.} \end{cases}$$

(2) *If k is odd, then*

$$[r, 1]_k = \begin{cases} 2 & \text{for } p = 2 \text{ and } r \in \Phi(\psi - 1),\ \psi \in \Phi \setminus \{1\}, \\ 1 & \text{for } p \neq 2 \text{ and } r \in \Phi(\psi - 1),\ \psi \in \Phi \setminus \{1\}, \\ 0 & \text{otherwise.} \end{cases}$$

In particular,

$$[1, 1]_k = \begin{cases} 2 & \text{for } p = 2 \text{ and } 3 \mid k, \\ 1 & \text{for } p \neq 2 \text{ and } 2 \in \Phi, \\ 0 & \text{otherwise.} \end{cases}$$

As all indices to $c_{j,i}$ occur as exponents of φ, they can be changed modulo k. Also notice that $i' = j - i$ if and only if $i = j - i'$. So we always can (and will) assume the representative is chosen from the set $\boldsymbol{k}_0$, even if e.g., $j - i'$ is not in this set.

Lemma 2.8 ([12, Lemma 9])**.** *Let (p,k) be circular, and let $\chi = (\psi - 1)^{-1}(\lambda - 1)$ where $\lambda, \psi \in \Phi \setminus \{1\}$. If $\chi \in \Phi$, then*

$$\textit{either} \quad \chi = 1 \quad \textit{and} \quad \psi = \lambda, \quad \textit{or} \quad \chi = -\lambda \quad \textit{and} \quad \psi = \lambda^{-1}.$$

The second case implies either $p = 2$, or that $|\Phi|$ is even.

We finish this subsection with the following facts. Recall from (3) that

$$A = \{\psi(\lambda - 1) \mid \psi, \lambda \in \Phi,\ \lambda \neq 1\}.$$

Lemma 2.9. *Let (p,k) be circular with k even. Then*

(1) $[2,1]_k = [-2,1]_k = 1$;

(2) $2\Phi = 2^{-1}\Phi \iff 2\Phi \cap 2^{-1}\Phi \neq \varnothing \iff 4 \in \Phi \iff [2^{-1},1]_k = 1$;

(3) $[2^{-1},1]_k = 2 \iff (2^{-1} \in A$ *and* $4 \notin \Phi)$.

Proof. In view of Lemma 2.7, and noticing that $-1 \in \Phi$, all implications in (1) and (2) are clear.

(3) By Lemma 2.7 we have $[2^{-1},1]_k = 2$ if and only if $2^{-1} \in A$ and $2^{-1} \notin 2\Phi$. As A is a union of cosets, all statements follow in view of (2). □

2.3. *Classification of overlaps*

In this subsection, we collect the notation, definitions, and key results from [11] that are needed to describe and classify overlaps among Φ-blocks. Central to this framework is the classification theorem ([11, Theorem 5.1]), which determines whether a given $c_{j,i}$ is involved in an overlap. These results will be used in Section 5 to analyze the cases listed in Table 1.

In the light of Theorem 2.3, a quadruple $(j, i \mid s, t)$, where $i, j, s, t \in \boldsymbol{k}$, $j \neq s$, is said to form an *overlap* (with respect to (F, Φ), or (q,k)) if

$$c_{j,i} = \varphi^{\omega} c_{s,t} \in \Phi c_{s,t} \quad \text{for some } \omega \in \boldsymbol{k}_0.$$

In this case, elements $b \in \Phi c_{j,i}$ are involved in an overlap.

Before turning to the general structure of overlaps, we first record the trivial cases, as noted in Remark 2.4. These are those $(j, i \mid s, t)$ with $j = i$, or $i = t$, or $s = k - j$. They are listed in [11, Table 3.1], which we record here for convenience:

$$\begin{cases} (j, j \mid s, s), & \\ (j, j \mid s, k-s) & \text{with } 2 \mid k \text{ or } p = 2, \\ (j,\ i \mid k-j, i) & \text{with } (2 \mid k \text{ or } p = 2) \text{ and } i \neq \frac{k}{2}, \\ (j,\ i \mid k-j, k-i) & \text{with } j \neq \frac{k}{2}. \end{cases} \tag{7}$$

The notion of overlap extends naturally beyond finite fields. In particular, it remains meaningful over the complex numbers $\mathbb{C}$, as there is always exactly one cyclic subgroup of $\mathbb{C}^*$ of order k. Denote by $\mathcal{O}(F,k)$ the set of all nontrivial overlaps over the field F, which by abuse of notation can also be $\mathbb{C}$.

The following theorem from [11] clarifies the relationship between overlaps over $\mathbb{C}$ and those over finite fields of characteristic p. By [11, Lemma 3.2], for a finite field F, $\mathcal{O}(F,k)$ depends only on the characteristic p of F; in this case, we can put $\mathcal{O}(p,k) = \mathcal{O}(F,k)$.

Theorem 2.10 ([11, Theorem 3.3]). *For a prime p, we have $\mathcal{O}(\mathbb{C},k) \subseteq \mathcal{O}(p,k)$. Moreover, for $k \geq 3$, the set $\mathcal{Q}_k = \{p \text{ prime} \mid p \text{ divides } k \text{ or } \mathcal{O}(\mathbb{C},k) \neq \mathcal{O}(p,k)\}$ is finite.*

Thus, if $p \notin \mathcal{Q}_k$ (in particular, if $p > \max \mathcal{Q}_k$), then $\mathcal{O}(p,k) = \mathcal{O}(\mathbb{C},k)$ and the classification theorems in [11] apply. This explains the frequent premise "$p \notin \mathcal{Q}_k$" in our theorems. Furthermore, this premise implies that (p,k) is circular. Indeed,

Theorem 2.11 ([11, Corollary 3.7]). *Let (p,k) be a Ferrero pair. If $p \notin \mathcal{Q}_k$, then (p,k) is circular.*

It may happen that $\Phi c_{j,i} = \Phi c_{s,t} = \Phi c_{s',t'}$, where j, s, and s' are distinct, and a *triple overlap* occurs. We denote this configuration by $(j,i \mid s,t \mid s',t')$. If none of the *constituent overlaps*—$(j,i \mid s,t)$, $(j,i \mid s',t')$, and $(s,t \mid s',t')$—is trivial, we say that $(j,i \mid s,t \mid s',t')$ is *nontrivial*.

We collect all nontrivial triple overlaps in the set $\mathcal{T} = \mathcal{T}(F,k)$, i.e.

$$\mathcal{T} = \{(s_1,t_1 \mid s_2,t_2 \mid s_3,t_3) \mid (s_1,t_1 \mid s_2,t_2), (s_2,t_2 \mid s_3,t_3), (s_1,t_1 \mid s_3,t_3) \in \mathcal{O}(F,k)\}.$$

We are interested in nontrivial overlaps only. So if $(s_1,t_1 \mid s_2,t_2 \mid s_3,t_3) \in \mathcal{T}$, we simply use the phrase "there is a triple overlap $(s_1,t_1 \mid s_2,t_2 \mid s_3,t_3)$," or "$(s_1,t_1 \mid s_2,t_2 \mid s_3,t_3)$ is a triple overlap", and the like to refer to a nontrivial triple overlap. Furthermore, nontrivial "quadruple" overlaps do not exist ([11, Corollary 7.5]).

We are going to wrap up the content of the two main theorems of overlaps, namely [11, Theorem 5.1] and [11, Theorem 7.4], into Theorem 2.13 below.

In order to understand the theorem, we need to discuss briefly the normalized form of an overlap. It follows from [11, Theorem 5.1] that a nontrivial overlap cannot occur when k is odd. Therefore we can assume that k is even.

Given an overlap $(s_1,t_1 \mid s_2,t_2)$ the following modification also give overlaps:

- replace any entry s by $k-s$;
- apply any of the following permutations to the entries (given in cycle form)

$$\begin{aligned}(s_1,t_2),\ (t_1,s_2),\ (s_1,t_2)(t_1,s_2),\ (s_1,s_2)(t_1,t_2),\\ (s_1,t_1)(s_2,t_2),\ (s_1,t_1,t_2,s_2),\ (s_1,s_2,t_2,t_1).\end{aligned} \tag{8}$$

Notice that not all transformed overlaps will be distinct. By [11, eq. (4.1)] in the list of all these transformed overlaps there will be one with

$$0 < s_1 < t_1 \leq s_2 < t_2 \leq \frac{k}{2}. \tag{9}$$

Such an overlap is called *normalized*. Only those are listed in the main theorem.

Similar transformations apply to triple overlaps, preserving their structural identity. This is formalized in the following lemma.

Lemma 2.12 ([11, Lemmas 7.1 & 7.2])**.** *We have*

$$\begin{aligned}(s_1, t_1 \mid s_2, t_2 \mid s_3, t_3) \in \mathcal{T} &\iff (s_2, t_2 \mid s_1, t_1 \mid s_3, t_3) \in \mathcal{T}\\ &\iff (s_3, t_3 \mid s_2, t_2 \mid s_1, t_1) \in \mathcal{T}\\ &\iff (t_1, s_1 \mid t_2, s_2 \mid t_3, s_3) \in \mathcal{T}.\end{aligned}$$

We are ready to present the classification theorem for overlaps. Notice that the non-trivial triple overlaps only occur if $30 \mid k$, and are placed where one of the constituents shows up inside $\mathcal{O}_{30}$.

Theorem 2.13 ([11, Theorem 5.1])**.** *Let $k \geq 3$ and $p \notin \mathcal{Q}_k$ such that $\mathcal{O}(p, k)$ is nonempty, then there exists $\ell \in \mathbb{N}$ such that $k = 6\ell$. Depending on the shape of k, $\mathcal{O}(p, k)$ is a union of the corresponding sets $\mathcal{O}_1$, $\mathcal{O}_{30}$, $\mathcal{O}_{42}$, and $\mathcal{O}_{60}$ described below. When we write $k = N\ell_r$ for $N \in \{30, 42, 60\}$, we mean that k is divisible by N with co-factor ℓ_r.*

(1) *For $k = 6\ell$, we have $\varphi^{\ell-i}\frac{\varphi^{\ell}-1}{\varphi^{i}-1} = \frac{\varphi^{3\ell-i}-1}{\varphi^{2i}-1}$ for $1 \leq i \leq \lfloor\frac{k}{4}\rfloor$, $i \neq \frac{k}{6} = \ell$, i.e., $\mathcal{O}_1$ consists of all normalized versions of all $(i, \ell \mid 2i, 3\ell - i)$, with $1 \leq i \leq \lfloor\frac{k}{4}\rfloor$ and $i \neq \frac{k}{6} = \ell$.*

(2) *For $k = 30\ell_1$, the normalized forms of the elements in $\mathcal{O}_{30}$ are*

$(\ell_1, 3\ell_1 \mid 3\ell_1, 11\ell_1)$ *with* $\omega = 3\ell_1$,		
$(3\ell_1, 5\ell_1 \mid 5\ell_1, 9\ell_1)$ *with* $\omega = \ell_1$,		$T_1 : (3\ell_1, 5\ell_1 \mid 5\ell_1, 9\ell_1 \mid 6\ell_1, 12\ell_1)$,
$(7\ell_1, 9\ell_1 \mid 9\ell_1, 13\ell_1)$ *with* $\omega = \ell_1$,		
$(\ell_1, 2\ell_1 \mid 4\ell_1, 9\ell_1)$ *with* $\omega = 2\ell_1$,		$T_2 : (\ell_1, 2\ell_1 \mid 4\ell_1, 9\ell_1 \mid 5\ell_1, 14\ell_1)$,
$(2\ell_1, 3\ell_1 \mid 5\ell_1, 8\ell_1)$ *with* $\omega = \ell_1$,		$T_3 : (2\ell_1, 3\ell_1 \mid 5\ell_1, 8\ell_1 \mid 7\ell_1, 14\ell_1)$,
		$T_4 : (2\ell_1, 5\ell_1 \mid 3\ell_1, 8\ell_1 \mid 4\ell_1, 13\ell_1)$,
$(8\ell_1, 9\ell_1 \mid 11\ell_1, 14\ell_1)$ *with* $\omega = \ell_1$,		$T_5 : (4\ell_1, 5\ell_1 \mid 8\ell_1, 11\ell_1 \mid 9\ell_1, 14\ell_1)$,
$(2\ell_1, 3\ell_1 \mid 7\ell_1, 14\ell_1)$ *with* $\omega = 3\ell_1$,		$T_3 : (2\ell_1, 3\ell_1 \mid 5\ell_1, 8\ell_1 \mid 7\ell_1, 14\ell_1)$,
$(3\ell_1, 4\ell_1 \mid 8\ell_1, 13\ell_1)$ *with* $\omega = 2\ell_1$,		$T_4 : (2\ell_1, 5\ell_1 \mid 3\ell_1, 8\ell_1 \mid 4\ell_1, 13\ell_1)$,
$(4\ell_1, 5\ell_1 \mid 9\ell_1, 14\ell_1)$ *with* $\omega = 2\ell_1$,		$T_2 : (\ell_1, 2\ell_1 \mid 4\ell_1, 9\ell_1 \mid 5\ell_1, 14\ell_1)$,
		$T_5 : (4\ell_1, 5\ell_1 \mid 8\ell_1, 11\ell_1 \mid 9\ell_1, 14\ell_1)$.

Here T_i, $i = 1, \ldots, 5$, are the nontrivial triple overlaps in normalized form.

(3) *For $k = 42\ell_2$, the normalized forms of the elements in $\mathcal{O}_{42}$ are*

$(2\ell_2, 3\ell_2 \mid 9\ell_2, 16\ell_2)$ *with* $\omega = 3\ell_2$,
$(3\ell_2, 4\ell_2 \mid 10\ell_2, 15\ell_2)$ *with* $\omega = 2\ell_2$,
$(8\ell_2, 9\ell_2 \mid 15\ell_2, 20\ell_2)$ *with* $\omega = 2\ell_2$.

(4) *For $k = 60\ell_3$, the normalized forms of the elements in $\mathcal{O}_{60}$ are*

$(3\ell_3, 4\ell_3 \mid 16\ell_3, 27\ell_3)$ *with* $\omega = 5\ell_3$,
$(5\ell_3, 6\ell_3 \mid 18\ell_3, 25\ell_3)$ *with* $\omega = 3\ell_3$,
$(8\ell_3, 9\ell_3 \mid 21\ell_3, 28\ell_3)$ *with* $\omega = 3\ell_3$.

As mentioned in the introduction, for a given $k \geq 3$, the set $\mathcal{Q}_k$ is a finite set of primes. There is another finite set $\mathcal{A}_k$ of primes, to be discussed in Section 4.3, satisfies $\mathcal{A}_k \subseteq \mathcal{Q}_k$ when $6 \mid k$ or $10 \mid k$, while in general $\mathcal{A}_k \subseteq \mathcal{Q}_{2k}$ for all $k \geq 3$. Let us briefly describe how $\mathcal{Q}_k$ and $\mathcal{A}_k$ can be computed.

So we have $k \geq 3$ given. Let $\phi = e^{2\pi i/k}$, a k-th primitive root of unity in $\mathbb{C}$. For all $i, j, s, t \in \boldsymbol{k}$ and $w \in \boldsymbol{k}_0$ with $i \neq s$ and $j \neq t$ set

$$u_{i,j,s,t,w} = \phi^w(\phi^i - 1)(\phi^t - 1) - (\phi^j - 1)(\phi^s - 1),$$

and compute the Galois norm $N_{i,j,s,t,w}$ of $u_{i,j,s,t,w}$ over $\mathbb{Q}$. Now if $u_{i,j,s,t,w} \neq 0$, and p is a prime dividing $N_{i,j,s,t,w}$, then

$$\varphi^w(\varphi^i - 1)(\varphi^s - 1) - (\varphi^j - 1)(\varphi^t - 1) = 0,$$

in a Galois field $F = \mathrm{GF}(q)$, where $\mathrm{char}F = p$ such that $k \mid (q-1)$, and φ a primitive k-th root of unity in F. This gives an overlap which has no corresponding overlap in $\mathbb{C}$, and so p is exceptional. The collection of all such primes makes $\mathcal{Q}_k$. Similarly, for $\mathcal{A}_k$, one compute the norm of all possible $v_{i,j,w} = \phi^w(\phi^i - 1)(\phi^j - 1) - 1$ with $i \neq j$, and collect the prime divisors of them when $v_{i,j,w} \neq 0$ or 1.

Table 2. Exceptional prime set $\mathcal{Q}_k$ for $3 \leq k \leq 16$

k	$\mathcal{Q}_k$	$\mathcal{A}_k$
3	$\{3\}$	$\{2, 7, 13\}$
4	$\{2, 3, 5\}$	$\{3, 5, 13, 17\}$
5	$\{5, 11\}$	$\{2, 11, 31, 41, 61, 71\}$
6	$\{2, 3, 5, 7, 13, 19, 31, 37\}$	$\{2, 3, 5, 7, 13, 19\}$
7	$\{2, 7, 13, 29, 43, 71\}$	$\{2, 13, 29, 43, 71, 113, 127, 197, 211\}$
8	$\{2, 3, 5, 7, 13, 17, 41, 73, 89, 97, 113\}$	$\{3, 5, 7, 13, 17, 41, 73, 97, 257\}$
9	$\{2, 3, 17, 19, 37, 73, 109, 127, 163, 181, 199, 271, 397, 541\}$	$\{2, 7, 13, 17, 19, 37, 73, 109, 127, (4^+), 757\}$
10	$\{2, 3, 5, 11, 19, 29, 31, 41, 61, 71, 101, 131, (16^+), 941\}$	$\{2, 3, 5, 11, 31, 41, 61, 71, 101, 211\}$
11	$\{3, 11, 23, 43, 67, 89, 109, 199, 331, 353, 397, (14^+), 2399\}$	$\{23, 67, 89, 199, 397, 617, 859, 1013, (7^+), 8009\}$
12	$\{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, (22^+), 1009\}$	$\{2, 3, 5, 7, 11, 13, 17, 19, 37, (5^+), 241\}$
13	$\{3, 5, 13, 53, 79, 103, 131, 157, 233, 313, (41^+), 24571\}$	$\{3, 53, 79, 131, 157, 313, 443, 521, (15^+), 39313\}$
14	$\{2, 3, 7, 13, 29, 41, 43, 71, 113, 127, 197, 211, (62^+), 24473\}$	$\{2, 3, 5, 13, 29, 43, 71, 113, 127, (7^+), 1009\}$
15	$\{2, 3, 5, 11, 19, 29, 31, 41, 59, 61, 71, 79, (143^+), 88411\}$	$\{2, 7, 11, 13, 19, 29, 31, 41, 61, (18^+), 4561\}$
16	$\{2, 3, 5, 7, 13, 17, 23, 31, 41, 47, 73, 79, 89, 97, (5^+), 257, (71^+), 102913\}$	$\{3, 5, 7, 13, 17, 41, 47, 73, 97, (12^+), 65537\}$
	(n^+) indicates that n values are omitted	

One can use the computer algebra program GAP [17] to compute the Galois norms readily when k is not too large (for example, $k \leq 100$). Also, one can use GAP to do prime factorization of the obtained norms to get $\mathcal{Q}_k$ and $\mathcal{A}_k$ easily when $k \leq 50$, say. As the norms are getting big when k is large, one may want to write the norms computed by GAP into a file, then use some number theoretic program like Pari/GP [18] for the task of factorizing. We provide $\mathcal{Q}_k$'s and $\mathcal{A}_k$'s for $3 \leq k \leq 16$ in Table 2 with longer sets truncated by showing the first twelve primes (except for $k = 16$) of $\mathcal{Q}_k$ and nine for that of $\mathcal{A}_k$, the number of omitted primes, and the last prime. Notice that $A_k \subseteq Q_{2k}$ $(3 \leq k \leq 8)$, illustrating the conjectural inclusion $A_k \subseteq Q_{2k}$ for all $k \geq 3$.

3. The case $x^m + by^m - bz^m = 1$, part I

Let $b \in F^*$ be fixed. As seen in the previous section, the set of solutions $(x, y, z) \in F^3$ to the equation

$$x^m + by^m - bz^m = 1, \tag{10}$$

splits into two disjoint subsets, denoted S and T. For certain circular Ferrero pair (F, Φ), we shall compute their cardinalities.

- In the first subsection (Counting S), the count for S governed by the coset $\Phi c_{i,j}$ containing b, together with whether the element $c_{i,j}$ is involved in overlap or not.
- In the second subsection (Counting T), the count for T the count is determined by whether b lies in A, in A^{-1}, in their intersection $A \cap A^{-1}$, or outside $A \cup A^{-1}$.

3.1. Counting S

Let us treat S first. From (4) we have that

$$|S| = m^3 \cdot \sum_{j=0}^{k-1} |(\Phi b + 1) \cap (\Phi b + \varphi^j)| = m^3 \cdot \left(k + \sum_{j=1}^{k-1} |(\Phi + b^{-1}) \cap (\Phi + \varphi^j b^{-1})| \right). \tag{11}$$

Thus, with

$$s_b = \sum_{j=1}^{k-1} |(\Phi + b^{-1}) \cap (\Phi + \varphi^j b^{-1})|,$$

we have

Theorem 3.1.

$$|S| = m^3 \cdot (k + s_b). \tag{12}$$

Recall the set

$$\mathcal{D} = \{\lambda(\varphi^j - 1)^{-1}(\varphi^i - 1) \mid \lambda \in \Phi,\ i, j \in \boldsymbol{k}\} = \cup_{i,j \in \boldsymbol{k}} \Phi c_{j,i},$$

and the facts $\mathcal{D} = \mathcal{D}^{-1} = -\mathcal{D}$ (c.f. Lemma 2.1). Thus, $s_b \neq 0$ precisely when there exists $j \in \boldsymbol{k}$ such that

$$(\Phi + b^{-1}) \cap (\Phi + \varphi^j b^{-1}) \neq \varnothing.$$

In this case,

$$(\Phi + \varphi^{k-j} b^{-1}) \cap (\Phi + b^{-1}) = \varphi^{k-j}((\Phi + b^{-1}) \cap (\Phi + \varphi^j b^{-1})) \neq \varnothing.$$

Lemma 2.2 says that this occurs if and only if $b^{-1} \in \mathcal{D}$. More precisely, we have

Lemma 3.2. *Let (F, Φ) be circular and $j \in \boldsymbol{k}$.*

(1) *If k is odd, then*

$$|(\Phi + b^{-1}) \cap (\Phi + \varphi^j b^{-1})| = \begin{cases} 2 & \text{if } p = 2 \text{ and } b^{-1} \in \Phi c_{j,i} \text{ for some } i \in \boldsymbol{k}, \\ 1 & \text{if } p \neq 2 \text{ and } b^{-1} \in \Phi c_{j,i} \text{ for some } i \in \boldsymbol{k}, \\ 0 & \text{otherwise.} \end{cases}$$

(2) *If k is even, then*

$$|(\Phi + b^{-1}) \cap (\Phi + \varphi^j b^{-1})| = \begin{cases} 2 & \text{if } b^{-1} \in \Phi c_{j,i},\ i \in \boldsymbol{k} \setminus \{\frac{k}{2}\}, \\ 1 & \text{if } b^{-1} \in \Phi c_{j,\frac{k}{2}}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. For $\chi, \psi \in \Phi$, we have $\chi + b^{-1} = \psi + \varphi^j b^{-1} \in (\Phi + b^{-1}) \cap (\Phi + \varphi^j b^{-1})$ if and only if

$$b^{-1} = \frac{\chi - \psi}{\varphi^j - 1} = \psi \frac{\chi\psi^{-1} - 1}{\varphi^j - 1} \in \Phi c_{j,i}, \quad \text{where } \chi\psi^{-1} = \varphi^i \text{ with } i \in \boldsymbol{k}.$$

Notice that $j \neq 0$ ensures $i \neq 0$. This already accounts for the "otherwise" case in both parts. So we assume that $b^{-1} \in \Phi c_{j,i}$. Then $(\Phi + b^{-1}) \cap (\Phi + \varphi^j b^{-1})$ is nonempty, and

$$\chi + b^{-1} = \psi + \varphi^j b^{-1},$$

for some $\chi, \psi \in \Phi$ with $\chi\psi^{-1} = \varphi^i$.

Set $r = \varphi^j b^{-1} - b^{-1} \neq 0$. By Lemma 2.6, we have

$$1 \leq |(\Phi + b^{-1}) \cap (\Phi + \varphi^j b^{-1})| = |\Phi \cap (\Phi + \varphi^j b^{-1} - b^{-1})| = [1, r]_k = [r, 1]_k.$$

If k is odd and $p \neq 2$, then $[r, 1]_k \leq 1$ by Lemma 2.7(2).

Now, assume that k is even or $p = 2$ (hence k is odd). Then $-1 \in \Phi$, and so

$$-\psi + b^{-1} = -\chi + \varphi^j b^{-1} \in (\Phi + b^{-1}) \cap (\Phi + \varphi^j b^{-1}).$$

Hence, except in the case $\psi = -\chi$, we have already two points of intersection. If $p = 2$, $\psi = -\chi = \chi$, which cannot happen. The odd case is done.

To finish the proof, we let k be even and $\psi = -\chi$ (so that $\chi\psi^{-1} = -1 = \varphi^{k/2}$), and claim that

$$|(\Phi + b^{-1}) \cap (\Phi + \varphi^j b^{-1})| = 1.$$

Suppose that this is not the case. Then there is another point $\lambda + b^{-1} = \mu + \varphi^j b^{-1}$ in the intersection, where $\lambda, \mu \in \Phi$ with $\lambda \neq \chi$ (hence $\mu \neq \psi$). Again, we have

$$-\mu + b^{-1} = -\lambda + \varphi^j b^{-1} \in (\Phi + b^{-1}) \cap (\Phi + \varphi^j b^{-1}).$$

From circularity, this has to be one of the two points in the intersection. Thus, either $\mu = -\lambda$ or $\mu = -\chi = \psi$. Our assumption rejects the later case. The former case gives $b^{-1} = \psi c_{j,\frac{k}{2}} = \mu c_{j,\frac{k}{2}}$, which still leads to $\psi = \mu$, and has to be rejected, too. Therefore, $|(\Phi + b^{-1}) \cap (\Phi + \varphi^j b^{-1})| = 1$ as claimed, and the proof is complete. □

Having set up the necessary preliminaries, we now examine the cases to determine s_b explicitly. Here is a summary of the outcomes.

Summary. In this subsection we determine the values of s_b. The outcome depends on the arithmetic position of $\pm b$ relative to the sets $\mathcal{D}$, together with the parity of k and the presence of overlaps or triple overlaps. The cases can be summarized as follows:

- (Theorem 3.3) If $\pm b \notin \mathcal{D}$, then $s_b = 0$.
- (Theorem 3.4) If k is odd and $\pm b \in \mathcal{D}$, then $s_b = 4$ or 2 depending on whether $p = 2$ or not.
- (Theorems 3.5 and 3.6) If k is even with $\pm b \in \Phi c_{i,j} \subseteq \mathcal{D}$, then:
  (1) If $k = 6$, or $3 \nmid k$, or if $c_{j,i}$ is not involved in an overlap, then $s_b = 2$ or 4 depending on whether $\frac{k}{2} \in \{i, j\}$.
  (2) If $k > 6$ and $6 \mid k$ with $c_{j,i}$ being involved in an overlap, then $s_b = 6$ if $\{i, j\} = \{\frac{k}{2}, \frac{k}{4}\}$, otherwise $s_b = 12$ or 8 depending on whether $c_{j,i}$ is involved in a triple overlap or not.

This roadmap allows us to move on to the formal case analysis. The overlap conditions will be clarified through A and A^{-1} in Section 4, and the solution counts will then be determined in Section 5 by the coset $\Phi(\varphi^i - 1)$ or $\Phi(\varphi^i - 1)^{-1}$ in which b lies.

We start with Theorem 3.3, which also includes the case $\pm b \in \Phi$ for completeness.

Theorem 3.3. *Suppose that (F, Φ) is circular and $b \in F^*$. Then*

(1) *If $\pm b \notin \mathcal{D}$, then $s_b = 0$.*

(2) *If $\pm b \in \Phi$, then*

$$s_b = \begin{cases} k - 1 & \text{if } k \text{ is odd, } p \neq 2, \\ 2k - 2 & \text{if } k \text{ is odd, } p = 2, \\ 2k - 3 & \text{if } k \text{ is even.} \end{cases}$$

Proof. (1) is a corollary to the previous lemma. (2) is essentially [12, Lemma 21]. □

Therefore, we are left with the case $\pm b \in (\mathcal{D} \setminus \Phi)$. This means that there exist $\psi \in \Phi$, $i, j \in \boldsymbol{k}$, $i \neq j$, and $i \neq k - j$, such that

$$b = \psi^{-1} \frac{\varphi^j - 1}{\varphi^i - 1} = \psi^{-1} c_{i,j} \quad \text{or, equivalently,} \quad b^{-1} = \psi \frac{\varphi^i - 1}{\varphi^j - 1} = \psi c_{j,i}. \tag{13}$$

Each of the $j \in \boldsymbol{k}$ to write b^{-1} in this form contributes to the sum s_b. Indeed, if also $b^{-1} = \chi c_{j',i'}$, with $j' \in \boldsymbol{k} \setminus \{j\}$, then there is an overlap $(j, i \mid j', i')$.

Let us settle the case when k is odd first.

Theorem 3.4. *Let (p, k) be a Ferrero pair with k odd $p \notin \mathcal{Q}_k$. If $b \in \mathcal{D} \setminus \Phi$, then*

$$s_b = \begin{cases} 4 & \text{if } p = 2, \\ 2 & \text{otherwise.} \end{cases}$$

Proof. Suppose $b \in \mathcal{D} = \mathcal{D}^{-1}$. Thus, $b^{-1} \in \Phi c_{j,i}$ for some $i, j \in \boldsymbol{k}$. Since $k - j \neq j$, both j and $k - j$ contribute to the sum for s_b. By Lemma 3.2, both terms are either 2 or 1 according to whether $p = 2$ or not. As there is no overlap involved, we have the result. □

From now on, we assume that k is even. Recall from Lemma 3.2 that whether i is $\frac{k}{2}$ (hence also whether j is $\frac{k}{2}$) make a difference.

Theorem 3.5. *Suppose that (p, k) is circular, and k is even. If $b \in \Phi c_{i,j}$, where $c_{i,j} \in \mathcal{D} \setminus (\Phi \cup -\Phi) = \mathcal{D} \setminus \Phi$ is not involved in an overlap, then we have*

$$s_b = \begin{cases} 2 & \text{if } i = \frac{k}{2} \text{ or } j = \frac{k}{2}, \\ 4 & \text{if } i \neq \frac{k}{2} \text{ and } j \neq \frac{k}{2}. \end{cases}$$

In particular, if $p \notin \mathcal{Q}_k$, then this is the case when $k = 6$, or $3 \nmid k$, or the pair (j, i) does not show up in the lists of Theorem 2.13.

Proof. In the case $i, j \notin \{\frac{k}{2}\}$, we have two nonzero terms in the sum defining s_b given by j and $k - j$. By Lemma 3.2 both terms are equal to 2.

If we have $i = \frac{k}{2}$ or $j = \frac{k}{2}$ (which cannot hold at the same time), we either have two terms with value 1, or just one term with value 2, respectively.

The special cases are all consequences of Theorem 2.13. □

For the next theorem we need to determine all nontrivial overlaps with $i = k/2$ or $j = k/2$. Suppose that $p \notin \mathcal{Q}_k$. Then

$$\left(\frac{k}{4}, \frac{k}{6} \,\middle|\, \frac{k}{2}, \frac{k}{4}\right) \quad \text{and} \quad \left(\frac{k}{6}, \frac{k}{4} \,\middle|\, \frac{k}{4}, \frac{k}{2}\right), \tag{14}$$

are two instances where $c_{\frac{k}{2},i}$ or $c_{j,\frac{k}{2}}$ $(i, j \in \boldsymbol{k})$ are involved in a nontrivial overlap. In these cases, it is necessary that $12 \mid k$. From Theorem 2.13, we see that these are the only instances where $\frac{k}{2}$ occurs. Thus, we have

Theorem 3.6. *Let (p, k) be a Ferrero pair. Suppose that $6 \mid k$ and $p \notin \mathcal{Q}_k$. Let $b \in \Phi c_{i,j}$, where $c_{i,j} \in (\mathcal{D} \setminus \Phi)$. If $c_{j,i}$ is involved in a nontrivial overlap, then we have*

$$s_b = \begin{cases} 6 & \text{if } 12 \mid k \text{ and } b \in \Phi c_{\frac{k}{4},\frac{k}{2}} \cup \Phi c_{\frac{k}{2},\frac{k}{4}}, \\ 12 & \text{if } c_{j,i} \text{ is involved in a nontrivial triple overlap}, \\ 8 & \text{otherwise}. \end{cases}$$

The conditions of the second and the third cases for s_b in the theorem will be made clear in Section 5, together with the counting of T.

3.2. Counting T

First we consider the case when two of the variables are zero.

Lemma 3.7. *Let n_0 be the number of those solutions of (10) having exactly two zero entries. Then*

$$n_0 = \begin{cases} 3m & \text{if } (2 \mid k \text{ or } p = 2) \text{ and } b \in \Phi, \\ 2m & \text{if } 2 \nmid k \text{ and } b \in \pm\Phi, \\ m & \text{if } b \notin \pm\Phi. \end{cases}$$

Proof. Observe that the equation $eX^m = 1$ over F admits a solution precisely when $e \in \Phi$. If this is the case, there are exactly m solutions. □

To count the rest of the elements in T, we recall

$$\begin{aligned} T_x &= \{(y,z) \in F^{*2} \mid by^m - bz^m = 1\} \quad \text{and} \quad \alpha_1 = |T_x|, \\ T_y &= \{(x,z) \in F^{*2} \mid \; x^m - bz^m = 1\} \quad \text{and} \quad \alpha_2 = |T_y|, \\ T_z &= \{(x,y) \in F^{*2} \mid \; x^m + by^m = 1\} \quad \text{and} \quad \alpha_3 = |T_z|. \end{aligned}$$

Note that T_x, T_y, and T_z are disjoint, and

$$|T| = \alpha_1 + \alpha_2 + \alpha_3 + n_0. \tag{15}$$

We define t_b as the number of elements in $\psi, \chi \in \Phi$ that satisfy $\psi - b\chi = 1$, and similarly for $t_{b^{-1}}$. Thus, in the notation of (6),

$$t_b = [b,1]_k = |\Phi \cap (\Phi b + 1)| \quad \text{and} \quad t_{b^{-1}} = [b^{-1},1]_k.$$

Then we have

Lemma 3.8. $\alpha_2 = \alpha_3 = t_b m^2$ *and* $\alpha_1 = t_{b^{-1}} m^2$.

Proof. We have

$$x^m + by^m = 1 \iff 1 + b(yx^{-1})^m = (x^{-1})^m \iff (x^{-1})^m - b(yx^{-1})^m = 1.$$

Thus $\alpha_2 = \alpha_3$. Since

$$x^m - bz^m = 1 \iff x^m \in \Phi \cap (\Phi b + 1),$$

and for each $c \in (\Phi b + 1)$, if there is a solution to the equation $x^m = c$, then there are exactly m solutions, we see that

$$\alpha_2 = |\{(x,z) \in F^{*2} \mid x^m - bz^m = 1\}| = t_b m^2.$$

Next,

$$by^m - bz^m = 1 \iff y^m = z^m + b^{-1} \iff y^m \in \Phi \cap (\Phi + b^{-1}).$$

Thus, using Lemma 2.6, we have $\alpha_1 = [1, b^{-1}]_k \cdot m^2 = [b^{-1}, 1]_k \cdot m^2 = t_{b^{-1}} m^2$. □

Combining the preceding lemmas, we can arrive at a general expression for $|T|$. The first two cases, corresponding to $\pm b \in \Phi$, were already established in our earlier work (see the introduction for references). For completeness we include them here in the statement. Only the 3rd case where $\pm b \notin \Phi$ requires further analysis.

Theorem 3.9. *If* (F,Φ) *is circular, then*

$$|T| = \begin{cases} 3t_1m^2 + 3m & \text{if } (2 \mid k \text{ or } p = 2) \text{ and } b \in \Phi, \\ 3t_1m^2 + 2m & \text{if } 2 \nmid k \text{ and } \pm b \in \Phi, \\ (2t_b + t_{b^{-1}})m^2 + m & \text{if } \pm b \notin \Phi. \end{cases} \tag{16}$$

Proof. In view of (15), the result is done with Lemmas 3.7 and 3.8 combined. The cases $b \in \Phi$ and $-b \in \Phi$ are covered by Lemma 2.6. Indeed, in these cases $t_b = t_{b^{-1}} = t_{-b} = t_1$. □

We now turn to the case $\pm b \notin \Phi$, where the term $2t_b + t_{b^{-1}}$ comes into play. Here, Lemma 2.7(1) provides the key to obtaining $2t_b + t_{b^{-1}}$ explicitly. First, let us recall the following notation from the introduction:

$$A = \{\psi(\chi - 1) \mid \chi, \psi \in \Phi, \chi \neq 1\} = \cup_{\chi \in \Phi\setminus\{1\}} \Phi(\chi - 1),$$
$$A^{-1} = \{\psi(\chi - 1)^{-1} \mid \chi, \psi \in \Phi, \chi \neq 1\} = \cup_{\chi \in \Phi\setminus\{1\}} \Phi(\chi - 1)^{-1},$$

and if $p \neq 2$,

$$2^{-1}\Phi = \{2^{-1}\chi \mid \chi \in \Phi\} = (2\Phi)^{-1}.$$

For completeness, we record the sizes of A and A^{-1}.

Lemma 3.10. *Let* (p,k) *be circular.*

$$|A| = |A^{-1}| = \begin{cases} k \cdot \frac{k}{2} & \text{if } k \text{ is even}, \\ k \cdot (k-1) & \text{if } k \text{ is odd}. \end{cases}$$

Proof. Clearly, $|A| = |A^{-1}|$. Let $\psi, \chi \in \Phi \setminus \{1\}$. By Lemma 2.8 we have $\psi - 1 \in \Phi(\chi - 1)$ if and only if $\psi = \chi$ when k is odd, or $\psi \in \{\chi, \chi^{-1}\}$ when k is even. Thus, the given number is verified for odd k. As for even k, there are $k - 2$ pairs χ and χ^{-1} in $\Phi \setminus \{\pm 1\}$, each pair gives one coset, while -1 gives one more coset. This completes the proof. □

We now return to the determination of $2t_b + t_{b^{-1}}$, where the sets A and A^{-1} play an important role.

As $t_b = [b, 1]_k$ and $t_{b^{-1}} = [b^{-1}, 1]_k$, the following theorem is a direct consequence of Lemma 2.7(2).

Theorem 3.11. *Let* (p,k) *be circular, with* k *odd and* $b \in F^*$. *Then*

$$2t_b + t_{b^{-1}} = \begin{cases} 3 & \text{if } b \in A \cap A^{-1}, \\ 2 & \text{if } b \in A \setminus A^{-1}, \\ 1 & \text{if } b \in A^{-1} \setminus A, \\ 0 & \text{otherwise}. \end{cases}$$

Remark 3.12. The theorem will be refined later in Corollary 4.17.

For the rest of this section we deal with the case when k is even. Here the analysis naturally splits into two parts: elements b lying in $2\Phi \cup 2^{-1}\Phi$, and those outside it. In this situation the coset 2Φ plays a central role. Since $-1 \in \Phi$, we have $2 = (-1)((-1)-1) \in A$. Therefore, $2\Phi \subseteq A$, and consequently,

$$A \setminus 2\Phi = \{\psi(\chi - 1) \mid \chi, \psi \in \Phi,\ \chi \neq \pm 1\}.$$

Moreover, by Lemma 2.7 we know that $t_b = 1$ if and only if $b \in 2\Phi$, and $t_b = 2$ if and only if $b \in A \setminus 2\Phi$.

With these preliminaries established, we begin with the first part of the even-k analysis, namely the situation when $b \in 2\Phi \cup 2^{-1}\Phi$.

Theorem 3.13. *Let (p, k) be circular, with k even, and $b \in 2\Phi \cup 2^{-1}\Phi$.*

(1) *If $2\Phi \cap 2^{-1}\Phi \neq \varnothing$ (thus, $2\Phi = 2^{-1}\Phi$ and $4 \in \Phi$), then $2t_b + t_{b^{-1}} = 3$.*

(2) *If $2\Phi \cap 2^{-1}\Phi = \varnothing$, then*

$$2t_b + t_{b^{-1}} = \begin{cases} 5 & \text{if } b \in 2^{-1}\Phi \text{ and } 2^{-1} \in A, \\ 4 & \text{if } b \in 2\Phi \text{ and } 2^{-1} \in A, \\ 2 & \text{if } b \in 2\Phi \text{ and } 2^{-1} \notin A, \\ 1 & \text{if } b \in 2^{-1}\Phi \text{ and } 2^{-1} \notin A. \end{cases}$$

Proof. All the ingredients we need are readily in Lemma 2.9.

Notice that if $b \in 2\Phi$, then $t_b = t_2 = 1$, and $b^{-1} \in 2^{-1}\Phi$. So

$$t_{b^{-1}} = t_{2^{-1}} = 1 \iff 2\Phi = 2^{-1}\Phi \iff 4 \in \Phi.$$

Now, when $2\Phi = 2^{-1}\Phi$, we have $2t_b + t_{b^{-1}} = 3$ which is (1).

If $2\Phi \cap 2^{-1}\Phi = \varnothing$, then $t_{b^{-1}} = 2 \iff 2^{-1} \in A$ and otherwise $t_{b^{-1}} = 0$. This accounts for all cases in (2) where $b \in 2\Phi$.

Finally, let $b \in 2^{-1}\Phi$, then $b^{-1} \in 2\Phi$, and $t_{b^{-1}} = t_2 = 1$. Similar as before:

$$t_b = t_{2^{-1}} = 2 \iff 2^{-1} \in A, \text{ and } t_b = 0 \text{ otherwise.}$$

This covers the remaining cases of (2). □

Now we handle the rest.

Theorem 3.14. *Let (p, k) be circular, with k even, and let $b \in F^* \setminus (2\Phi \cup 2^{-1}\Phi)$. Then*

$$2t_b + t_{b^{-1}} = \begin{cases} 6 & \text{if } b \in A \cap A^{-1}, \\ 4 & \text{if } b \in A \setminus A^{-1}, \\ 2 & \text{if } b \in A^{-1} \setminus A, \\ 0 & \text{if } b \notin A \cup A^{-1}. \end{cases}$$

Proof. We apply Lemma 2.7(1) directly. If $b \notin A \cup A^{-1}$, then the sum is 0.

If $b \in A$, then $t_b = 2$ and if $b^{-1} \in A$, then $t_{b^{-1}} = 2$, and both values are zero otherwise, as $2\Phi \cup 2^{-1}\Phi$ is not considered. This completes the proof of the theorem. □

Thus the evaluation of $2t_b + t_{b^{-1}}$ is complete: for odd k the values are given in Theorem 3.11, and for even k it is covered by Theorems 3.13 and 3.14.

4. The sets A, A^{-1}, and $A \cap A^{-1}$

The theorems in the previous section show that the sets A and A^{-1}, together with their intersection $A \cap A^{-1}$, play a central role in determining the number of solutions to the equation $x^m + by^m - bz^m = 1$ over the finite field F.

The main objective of this section is to characterize $A \cap A^{-1}$. Our principal result is Theorem 4.11. Although the statements are formulated over $\mathbb{C}$, they remain valid over finite fields provided that the characteristic of F lies outside the exceptional set $\mathcal{Q}_k$ and that $6 \mid k$ or $10 \mid k$.

Observe that when k is even, the characteristic $p = \mathrm{char}(F)$ is odd, so $2 \neq 0$ in F. In many cases we will assume $6 \mid k$. Then the subgroup Φ contains the element $\rho = \varphi^{\frac{k}{6}}$, which has order 6. Being a primitive 6th root of unity, ρ satisfies the relation $\rho^2 - \rho + 1 = 0$. This notation will be used freely throughout this section whenever appropriate.

4.1. Structural Properties of A, A^{-1}, and $\mathcal{D}$

We begin with the case of even k, leaving the odd case to the next subsection.

When k is even we have $2\Phi \subseteq A$. For, if $\psi \in \Phi$, then $-1, -\psi \in \Phi$, and so $2\psi = -\psi(-1-1) \in A$.

Lemma 4.1. *Let k be even and $i \in \boldsymbol{k} \setminus \{\frac{k}{2}\}$. Then $\varphi^i - 1 \in \Phi c_{\frac{k}{2}+i, 2i}$. Consequently, $(A \setminus 2\Phi) \subseteq \mathcal{D}$ and $(A^{-1} \setminus 2^{-1}\Phi) \subseteq \mathcal{D}$.*

If $6 \mid k$, then $\{2, -2\} \subseteq \Phi c_{\frac{k}{6}, \frac{k}{2}}$, and $\{2^{-1}, -2^{-1}\} \subseteq \Phi c_{\frac{k}{2}, \frac{k}{6}}$. Therefore, in this case, $(A \cup A^{-1}) \subseteq \mathcal{D}$.

Proof. For the first statement, as $i \neq \frac{k}{2}$, we have $\varphi^i \neq -1$. For $\lambda \in \Phi$,

$$\lambda(\varphi^i - 1) = \lambda(\varphi^i + 1)^{-1}(\varphi^{2i} - 1) = (-\lambda)(\varphi^{\frac{k}{2}+i} - 1)^{-1}(\varphi^{2i} - 1) \in \Phi c_{\frac{k}{2}+i, 2i} \subseteq \mathcal{D}.$$

Thus, $(A \setminus 2\Phi) \subseteq \mathcal{D}$. Similarly, $(A^{-1} \setminus 2^{-1}\Phi) \subseteq \mathcal{D}$.

If $6 \mid k$, then $(\varphi^{\frac{k}{6}})^3 = -1$, so $\varphi^{\frac{k}{6}} - 1 = (\varphi^{\frac{k}{6}})^2 = \varphi^{\frac{k}{3}}$. Hence

$$-2 = \varphi^{\frac{k}{2}} - 1 = \varphi^{\frac{2k}{3}}(\varphi^{\frac{k}{6}} - 1)^{-1}(\varphi^{\frac{k}{2}} - 1) \in \Phi c_{\frac{k}{6}, \frac{k}{2}} \subseteq \mathcal{D},$$

and therefore $\{2, -2\} \subseteq \Phi c_{\frac{k}{6}, \frac{k}{2}}$, which implies $2\Phi \subseteq \mathcal{D}$ and thus $A \subseteq \mathcal{D}$. Similarly, $-2^{-1} = (-2)^{-1} \in \Phi c_{\frac{k}{2}, \frac{k}{6}} \subseteq \mathcal{D}$, so $\{2^{-1}, -2^{-1}\} \subseteq \Phi c_{\frac{k}{2}, \frac{k}{6}}$, which yields $2^{-1}\Phi \subseteq \mathcal{D}$, and hence $A^{-1} \subseteq \mathcal{D}$. □

Remark 4.2. The case $\varphi^{\frac{k}{2}} - 1 = -2$ for even k is excluded from Lemma 4.1 except when $6 \mid k$. In fact, ensuring $-2 \in \mathcal{D}$ essentially requires $6 \mid k$. This subtlety, together with the relation between A and $\mathcal{D}$ when k is odd, will be revisited in the next subsection, where we analyze the situation over the complex field $\mathbb{C}$.

In many situation, Φ sits inside $A \cap A^{-1}$.

Lemma 4.3. *Let $6 \mid k$. Then for $s \in \boldsymbol{k}$ we have*

$$\varphi^s - 1 \in \Phi \iff s \in \{\tfrac{k}{6}, \tfrac{5k}{6}\}.$$

In particular, since $\varphi^{\frac{k}{6}} - 1 \in \Phi$, it follows that $\Phi \subseteq (A \cap A^{-1})$.

Proof. We write $k = 6\ell$. As $\varphi^\ell = \rho$, we obtain $\varphi^\ell - 1 = \rho - 1 = \rho^2 \in \Phi$. Therefore if $\varphi^s - 1 \in \Phi$, then $c_{\ell,s} = \frac{\varphi^s-1}{\varphi^\ell-1} \in \Phi$. By Lemma 2.5 this forces $s = \ell = \frac{k}{6}$ or $s = k - \ell = \frac{5k}{6}$. $\square$

We we have seen in Theorem 2.13 that a nontrivial overlap can only occur when $6 \mid k$. In this case, many of the occurrences of overlaps are related to elements in $A \cup A^{-1}$.

First, we notice that when $6 \mid k$, certain cosets $\Phi(\varphi^i - 1)$, $1 \le i \le k-1$, collapse. In this case, a primitive 6th root of unity $\rho = \varphi^{\frac{k}{6}}$ lies in Φ. This immediately gives the following collapsing identities

$$2\Phi = \Phi(\rho^3 - 1), \qquad \Phi = \Phi(\rho - 1) = \Phi(\rho^5 - 1), \qquad \Phi(\rho^2 - 1) = \Phi(\rho^4 - 1). \tag{17}$$

Now, the following lemma says that every element in A which is not in $\cup_{t=1}^5 \Phi(\rho^t - 1)$ is involved in an overlap; likewise, every element in A^{-1} which is not in $\cup_{t=1}^5 \Phi(\rho^t - 1)^{-1}$ is involved in an overlap.

Lemma 4.4. *Let $6 \mid k$ and $g \in F^*$.*

(1) *If $g \in \Phi(\varphi^i - 1)$ with $1 \le i < \frac{k}{2}$, then $g \in \Phi c_{\frac{k}{6},i} = \Phi c_{\frac{k}{2}-i,2i}$.*

(2) *If $g \in \Phi(\varphi^i - 1)^{-1}$ with $1 \le i < \frac{k}{2}$, then $g \in \Phi c_{i,\frac{k}{6}} = \Phi c_{2i,\frac{k}{2}-i}$.*

Here, $\Phi c_{\frac{k}{6},i} = \Phi c_{\frac{k}{2}-i,2i}$ and $\Phi c_{i,\frac{k}{6}} = \Phi c_{2i,\frac{k}{2}-i}$ are nontrivial overlaps unless $i \in \{\frac{k}{6}, \frac{k}{3}\}$.

Proof. Write $k = 6\ell$. By symmetry it suffices to prove (1), and it is enough to consider $g = \varphi^i - 1$. Using $\varphi^{3\ell} = -1 = \varphi^{-3\ell}$ and $\varphi^\ell - 1 = \varphi^{2\ell}$ we compute

$$\varphi^i - 1 = (-1)(\varphi^{3\ell+i} + 1) = (-1)\frac{\varphi^{2(3\ell+i)} - 1}{\varphi^{3\ell+i} - 1} = \frac{\varphi^{2i} - 1}{1 - \varphi^{3\ell+i}}.$$

Now, from

$$\frac{\varphi^{2i} - 1}{1 - \varphi^{3\ell+i}} = \varphi^{3\ell-i}\frac{\varphi^{2i} - 1}{\varphi^{3\ell-i} - 1} \in \Phi c_{3\ell-i,2i},$$

and

$$\frac{\varphi^{2i} - 1}{1 - \varphi^{3\ell+i}} = \varphi^{2\ell}\frac{\varphi^i - 1}{\varphi^\ell - 1} \in \Phi c_{\ell,i},$$

we see that we have an overlap $(\ell, i \mid 3\ell - i, 2i)$. Except for $i \in \{\ell, 2\ell\}$, which gives trivial overlaps, this overlap is a member of $\mathcal{O}_1$. $\square$

Remark 4.5. (1) Theorem 2.13 lists all nontrivial possible overlaps in their normalized forms. The theorem indicates that a nontrivial overlap can occur only when k is even and is divisible by 3, 5 or 7. We shall see later in Theorem 4.11 that if $A \cap A^{-1} \neq \varnothing$, then k has to be divisible by 3 or 5. Moreover, the structure of $A \cap A^{-1}$ will be determined there.

(2) Note that $A \cup A^{-1}$ does not cover all elements of F^* which are involved in overlaps. For example, for $k = 30\ell_1$, $\ell_1 \in \mathbb{N}$, $(\ell_1, 3\ell_1 \mid 3\ell_1, 11\ell_1)$ is an overlap and $c_{\ell_1, 3\ell_1}$ is not a member of $A \cup A^{-1}$.

(3) Though the condition $i \leq \frac{k}{4}$ seems violated in the specific overlap $(i, \ell \mid 2i, 3\ell - i)$, it is still legitimately a member of $\mathcal{O}_1$. Indeed, if $i > \frac{k}{2}$, then $\varphi^i - 1 = (\varphi^{k-i} - 1)(-\varphi^i)$. Thus $\varphi^i - 1$ and $\varphi^{k-i} - 1$ belong to the same coset of Φ (cf. Lemma 2.8), allowing us to restrict to $i < \frac{k}{2}$. Notice that $i = \frac{k}{2}$ is not possible as $2i$ must be in $\boldsymbol{k}$. Transformations like this and in the following paragraph are explained in (8) and lead to the normalized form (9).

Furthermore, if $\frac{k}{4} < i < \frac{k}{2}$, then we put $j = 3\ell - i = \frac{k}{2} - i < \frac{k}{4}$ and we obtain $(i, \ell \mid 2i, 3\ell - i) = (3\ell - j, \ell \mid k - 2j, j)$. As in the first part we can transform this into the overlap $(3\ell - j, \ell \mid 2j, j)$. Therefore $\frac{\varphi^\ell - 1}{\varphi^{3\ell - j} - 1}\Phi = \frac{\varphi^j - 1}{\varphi^{2j} - 1}\Phi$, which is equivalent to $\frac{\varphi^{3\ell - j} - 1}{\varphi^\ell - 1}\Phi = \frac{\varphi^{2j} - 1}{\varphi^j - 1}\Phi$. This last overlap reads in shorthand: $(j, 2j \mid \ell, 3\ell - j)$ with $j < \frac{k}{4}$.

To facilitate the analysis of $A \cap A^{-1}$, we now assume for the rest of this section that F is an arbitrary field having a subgroup Φ of F^* of order k. In particular, F is not necessarily finite.

To begin with, we'll give examples for subsets in $A \cap A^{-1}$.

Theorem 4.6. *Let F be an arbitrary field and assume k to be even.*

(1) $2^{-1} \in A$ *if and only if* $2\Phi \cup 2^{-1}\Phi \subseteq (A \cap A^{-1})$. *Otherwise* $(2\Phi \cup 2^{-1}\Phi) \cap (A \cap A^{-1}) = \varnothing$.

(2) *If* $6 \mid k$, *then* $\Phi \subseteq (A \cap A^{-1})$.

(3) *If* $10 \mid k$, *then* $\Phi(\zeta - 1) \cup \Phi(\zeta^3 - 1) \subseteq (A \cap A^{-1})$, *where* $\zeta \in \Phi$ *is of order* 10.

(4) *If* $12 \mid k$, *then* $\Phi(\sigma - 1) \cup \Phi(\sigma^5 - 1) \subseteq (A \cap A^{-1})$, *where* $\sigma \in \Phi$ *is of order* 12.

While $2\Phi = 2^{-1}\Phi$ *is possible, the cosets in (3) and (4) are distinct.*

Proof. (1) The first part is immediate. The complementary case follows since $A \cap A^{-1}$ is a union of cosets of Φ.

(2) This is already in Lemma 4.3, where the proof does not require F to be finite.

(3) The 10th cyclotomic polynomial reads $x^4 - x^3 + x^2 - x + 1$. Thus,

$$(\zeta - 1)(\zeta^3 - 1) = \zeta^4 - \zeta^3 - \zeta + 1 = -\zeta^2 \in \Phi,$$

which implies

$$\Phi(\zeta - 1) = \Phi(\zeta^3 - 1)^{-1} \subseteq (A \cap A^{-1}), \qquad \Phi(\zeta^3 - 1) = \Phi(\zeta - 1)^{-1} \subseteq (A \cap A^{-1}).$$

(4) The 12th cyclotomic polynomial reads $x^4 - x^2 + 1$. Using $\sigma^6 = -1$,

$$(\sigma - 1)(\sigma^5 - 1) = \sigma^6 - \sigma^5 - \sigma + 1 = -\sigma(\sigma^4 + 1) = -\sigma^3 \in \Phi,$$

and the claim follows as in (3).

The final statement is a consequence of Lemma 2.8. □

Remark 4.7. In the theorem, we have

$$\Phi(\zeta - 1) = \Phi(\zeta^{-1} - 1), \qquad \Phi(\zeta^3 - 1) = \Phi(\zeta^{-3} - 1).$$

Thus the choice of ζ among the four possible elements of order 10 in Φ makes no difference. The same applies to σ of order 12. This symmetry ensures that the coset structure is invariant under inversion, reinforcing the stability of $A \cap A^{-1}$ under group automorphisms.

Now, $u \in A \cap A^{-1}$ if and only if $u = \varphi^s(\varphi^i - 1) = \varphi^t(\varphi^j - 1)^{-1}$ for some $i, j \in \boldsymbol{k}$ and $s, t \in \boldsymbol{k}_0$. This implies

$$(\varphi^i - 1)(\varphi^j - 1) = \varphi^{i+j} - \varphi^i - \varphi^j + 1 = \varphi^{t-s} \in \Phi. \tag{18}$$

4.2. The complex case

In this subsection, we investigate in $\mathbb{C}$ the relation between A and $\mathcal{D}$ and the structure of $A \cap A^{-1}$.

Assume for this subsection that $F = \mathbb{C}$, the field of complex numbers. Let $S^1 = \{e^{\theta \boldsymbol{i}} \mid \theta \in \mathbb{R}\}$ denote the unit circle. Put $\phi = e^{2\pi i/k}$, and we have $\Phi = \langle \phi \rangle \subseteq S^1$.

First of all, it is worth noting that when k is odd, A and $\mathcal{D}$ has nothing in common.

Lemma 4.8. *If k is odd, then $\mathcal{D} \cap A = \varnothing$. In particular, $\Phi \cap A = \varnothing$.*

Proof. Suppose that $g \in \mathcal{D} \cap A$. So $g = \phi^w \frac{\phi^i - 1}{\phi^j - 1} = \phi^s(\phi^t - 1)$, $i \neq k$, $j \neq k$, $t \neq k$. We may assume that $s = 1$. Using

$$\phi^\ell - 1 = \phi^{\ell/2}\left(\phi^{\ell/2} - \phi^{-\ell/2}\right) = \phi^{\ell/2} 2\boldsymbol{i} \sin(\tfrac{2\pi}{2k}\ell) \quad \text{for any } \ell \in \{1, 2, \ldots, k\},$$

we find

$$\phi^w \frac{\phi^u - 1}{\phi^j - 1} = \phi^t - 1 \iff \phi^{w + \frac{u}{2} - \frac{j}{2} - \frac{t}{2}} \frac{\sin(\frac{2\pi}{2k}u)}{\sin(\frac{2\pi}{2k}j)} = 2\boldsymbol{i} \sin\left(\tfrac{2\pi}{2k}t\right).$$

As all the sines are real

$$\phi^{w + \frac{u}{2} - \frac{j}{2} - \frac{t}{2}} = \pm \boldsymbol{i}.$$

Therefore

$$w + \tfrac{u}{2} - \tfrac{j}{2} - \tfrac{t}{2} \in \{\tfrac{k}{4}, \tfrac{3k}{4}\} \iff 4w + 2u - 2j - 2t \in \{k, 3k\},$$

which implies that k is even. □

Next, let us return to the case that k is even and $i = \frac{k}{2}$ in Lemma 4.1 over $\mathbb{C}$.

Lemma 4.9. *If $\Phi(\phi^{\frac{k}{2}} - 1) \subseteq \mathcal{D}$, then $6 \mid k$.*

Proof. Assume that $\Phi(\phi^{\frac{k}{2}} - 1) \subseteq \mathcal{D}$. With $\phi^{\frac{k}{2}} - 1 = -2$, this means that $-2 = \phi^s(\phi^i - 1)^{-1}(\phi^j - 1)$ for some $i, j \in \boldsymbol{k}$ and $s \in \boldsymbol{k}_0$. Therefore,

$$-2\phi^i + 2 = \phi^{s+j} - \phi^s,$$

which gives a vanishing sum of roots of unity of length 6 (cf. [2]):

$$\phi^{\frac{k}{2}+i} + \phi^{\frac{k}{2}+i} + 1 + 1 + \phi^{\frac{k}{2}+s+j} + \phi^s = 0.$$

As there are two 1's and two $\phi^{\frac{k}{2}+i}$'s, one infers easily from [2, Theorem 6] that $\phi^{\frac{k}{2}+i}$, $\phi^{\frac{k}{2}+s+j}$ and $\phi^{\frac{k}{2}+s}$ has to be 3rd root of unity. Thus $3 \mid k$, and since k is even, it follows that $6 \mid k$. □

For further discussions, we also recall a part of [2, Theorem 7]. It is recorded here for the convenience of the readers.

Theorem 4.10. *Suppose we have at most two distinct rational multiples of π lying strictly between 0 and $\frac{\pi}{2}$ for which some rational linear combination of their cosines is rational but no proper subset has this property. Then the appropriate linear combination is proportional to one from the following list:*

$$\cos\frac{\pi}{3} = \frac{1}{2}, \tag{19}$$

$$\cos\frac{\pi}{5} - \cos\frac{2\pi}{5} = \frac{1}{2}. \tag{20}$$

We have

Theorem 4.11. *Let $F = \mathbb{C}$. If $A \cap A^{-1} \neq \varnothing$ then $3 \mid k$ or $5 \mid k$. In particular*

(1) *If k is odd, then $A \cap A^{-1} = \varnothing$.*

(2) *If $\gcd(30, k) = 10$, then*

$$A \cap A^{-1} = \Phi(\zeta - 1) \cup \Phi(\zeta^3 - 1),$$

where $\zeta \in \Phi$ is of order 10.

(3) *If $\gcd(60, k) = 6$, then $A \cap A^{-1} = \Phi$.*

(4) *If $\gcd(60, k) = 12$, then*

$$A \cap A^{-1} = \Phi \cup \Phi(\sigma - 1) \cup \Phi(\sigma^5 - 1),$$

where $\sigma \in \Phi$ is of order 12.

(5) *If $\gcd(60, k) = 30$, then*

$$A \cap A^{-1} = \Phi \cup \Phi(\zeta - 1) \cup \Phi(\zeta^3 - 1),$$

where $\zeta \in \Phi$ is of order 10.

(6) *If* $60 \mid k$, *then*

$$A \cap A^{-1} = \Phi \cup \Phi(\zeta - 1) \cup \Phi(\zeta^3 - 1) \cup \Phi(\sigma - 1) \cup \Phi(\sigma^5 - 1),$$

where $\zeta, \sigma \in \Phi$ *are of order* 10 *and* 12, *respectively.*

Proof. Theorem 4.6 covers the inclusion "$\supseteq$" in all cases. For the other inclusion, we first do the case when k is even.

Recall that Φ is generated by ϕ and we can assume that $\phi = e^{2\pi i/k}$. From (18), we see that if $A \cap A^{-1} \neq \varnothing$, then there are i and j such that

$$\phi^{i+j} - \phi^i - \phi^j + 1 \in \Phi, \tag{21}$$

Replacing ϕ^i by ϕ^{-i} and/or ϕ^j by ϕ^{-j} and recalling that $-1 \in \Phi$ there is no loss to assume $0 < i \leq j \leq \frac{k}{2}$. Put $t = \frac{i+j}{2}$ and $s = \frac{j-i}{2}$, then

$$0 < t \leq \frac{k}{2},\ 0 \leq s < \frac{k}{4},\ i = t - s,\ j = t + s.$$

Now the condition reads $\phi^{2t} - \phi^{t-s} - \phi^{t+s} + 1 \in \Phi$. We multiply by ϕ^{-t} to obtain

$$\phi^t - \phi^{-s} - \phi^s + \phi^{-t} \in \Phi\phi^{-t},$$

hence

$$2\cos\frac{2\pi}{k}t - 2\cos\frac{2\pi}{k}s \in \Phi\phi^{-t} \subseteq S^1.$$

Note the left hand side is real, and $\Phi\phi^{-t}$ contains real numbers if and only if $\phi^{-t} \in \Phi$. In this case these real numbers can only be ± 1. Moreover, t and thus s are integers, which satisfy $s < t$. As cosine is strictly decreasing on the interval $[0, \pi]$, we arrive at

$$\cos\frac{2\pi}{k}t - \cos\frac{2\pi}{k}s = -\frac{1}{2}.$$

We begin by applying Theorem 4.10 to the case when $t \leq \frac{k}{4}$. This gives three cases, where the first two come from (19) with 0 or 1 added, and the last from (20).

(a) $s = 0$, then $t = \frac{k}{6}$, so $6 \mid k$, thus $i = j = \frac{k}{6}$;

(b) $t = \frac{k}{4}$, then $s = \frac{k}{6}$, so $12 \mid k$, thus $i = \frac{k}{12}$ and $j = \frac{5k}{12}$;

(c) $t = \frac{k}{5}$, then $s = \frac{k}{10}$, so $10 \mid k$, thus $i = \frac{k}{10}$ and $j = \frac{3k}{10}$.

These three cases correspond to the minimal cyclotomic configurations that yield rational cosine combinations, and thus determine when $A \cap A^{-1} \neq \varnothing$.

If $t > \frac{k}{4}$ put $t' = \frac{k}{2} - t$ and the expression transforms into

$$\cos\frac{2\pi}{k}t' + \cos\frac{2\pi}{k}s = \frac{1}{2} \quad \text{as} \quad \cos(\pi - x) = -\cos x.$$

But then $\{t', s\}$ is $\{\frac{k}{10}, \frac{3k}{10}\}$ or $\{\frac{k}{4}, \frac{k}{6}\}$ which contradicts the facts that both $t' < \frac{k}{4}$ and $s < \frac{k}{4}$.

This covers all the cases (2)–(6).

Hence we're left with the odd k case. Then Φ is a subgroup of the group Ψ of order $2k$ and there exists a generator ψ of Ψ with $\varphi = \psi^2$. Assume there are i and j with satisfying (21). Then we obtain

$$\psi^{2i+2j} - \psi^{2i} - \psi^{2j} - 1 \in \Phi \subseteq \Psi.$$

But the configurations in (a)–(c) all require even k, yielding a contradiction.

This covers the rest of the theorem. □

This completes the classification of $A \cap A^{-1}$ over the complex field $\mathbb{C}$. The divisibility conditions $3 \mid k$ and $5 \mid k$ arise precisely from the minimal cyclotomic configurations identified in Theorem 4.10. Such structural classification under gcd conditions will serve a purpose in Section 5, where it validates the enumerations of N_b recorded in Table 1. In the next subsection we turn to finite fields, where analogous structures appear under suitable restrictions on the characteristic.

4.3. Finite field analogues of $A \cap \mathcal{D}$ and $A \cap A^{-1}$

Coming back to finite fields, we let (p, k) be a Ferrero pair.

For every solution of eq. (21) there exist $i, j \in \boldsymbol{k}$ and $s \in \boldsymbol{k}_0$, such that φ is a zero of the polynomial

$$\begin{aligned} f_{s,i,j}(x) &= x^s(x^i - 1)(x^j - 1) - 1 \\ &= x^{s+i+j} - x^{s+i} - x^{s+j} + x^s - 1. \end{aligned}$$

Thus there is an element in $A \cap A^{-1}$ if and only if $f_{s,i,j}(\varphi) = 0$ for some $s \in \boldsymbol{k}_0$ and $i, j \in \boldsymbol{k}$.

Solutions as described over $\mathbb{C}$ in Theorem 4.11 correspond to solutions over finite fields—except when the characteristic lies in a finite exceptional set $\mathcal{A}_k$. However, there can be more solutions over a finite field F. Just like $\mathcal{P}_k$ and $\mathcal{Q}_k$, there is a finite set $\mathcal{A}_k$ of exceptional primes with the property that this can only happen if the characteristic of F is in $\mathcal{A}_k$. For all other characteristics the solutions correspond exactly to those over $\mathbb{C}$ (cf. [11]).

To find $\mathcal{A}_k$, one may use [11, Prop. 3.4] as in the proof of [11, Theorem 3.3], and show

Lemma 4.12. *Let ϕ be a primitive kth root of unity in $\mathbb{C}$ and $\mathcal{N} : \mathbb{Q}[\phi] \to \mathbb{Q}$ be the Galois norm. Then*

$$\begin{aligned} \mathcal{A}_k = \{p \mid p \text{ a prime divisor of } \mathcal{N}(f_{s,i,j}(\phi)) \text{ for } s \in \boldsymbol{k}_0,\ i, j \in \boldsymbol{k},\ \mathcal{N}(f_{s,i,j}(\phi)) \neq 0\} \\ \cup \{p \text{ is a prime divisor of } k\}. \end{aligned}$$

In particular, $\mathcal{A}_k$ is finite.

The following lemma is the key for us to use Theorem 4.11 in the context of finite fields.

Lemma 4.13. *If $6 \mid k$ or $10 \mid k$, then $\mathcal{A}_k \subseteq \mathcal{Q}_k$.*

Proof. Let $i, j \in \boldsymbol{k}$ and $s \in \boldsymbol{k}_0$ such that

$$\phi^s(\phi^i - 1)(\phi^j - 1) - 1 = 0.$$

Then

$$\phi^s(\phi^i - 1)(\phi^j - 1) = 1.$$

Suppose that $6 \mid k$, and write $k = 6\ell$. Then ϕ^ℓ is a primitive sixth root of unity, thus $\phi^{2\ell} - \phi^\ell + 1 = 0$. Using $\phi^{3\ell} = -1$, one can derive $(\phi^{5\ell} - 1)(\phi^\ell - 1) = 1$. From (18), we know that there is some $s \in \boldsymbol{k}_0$ such that

$$\phi^s(\phi^i - 1)(\phi^j - 1) - 1 = 0.$$

Therefore,

$$\phi^s(\phi^i - 1)(\phi^j - 1) - (\phi^{5\ell} - 1)(\phi^\ell - 1) = 0,$$

which is an equation that shows up with overlaps. As in the proof of [11, Corollary 3.7] one can see that each prime from $\mathcal{A}_k$ is also in $\mathcal{Q}_k$.

Similarly, when $k = 10\ell$, using $\phi^{-2\ell}(\phi^\ell - 1)(\phi^{3\ell} - 1) = -1$, we see that each prime from $\mathcal{A}_k$ is also in $\mathcal{Q}_k$. □

Remark 4.14. Supported by data, we conjecture that for all k we have $\mathcal{A}_k \subseteq \mathcal{Q}_{2k}$. A proof in the case that k is odd with $3 \mid k$ or $5 \mid k$ is easy: Clearly, $\mathcal{A}_k \subseteq \mathcal{A}_{2k}$, and we know from Lemma 4.13 $\mathcal{A}_{2k} \subseteq \mathcal{Q}_{2k}$.

Now, with Lemma 4.9, we can sharpen Lemma 4.1.

Lemma 4.15. *Let $p \notin \mathcal{Q}_k \cup \mathcal{A}_k$. If k is even and $i \in \boldsymbol{k} \setminus \{\frac{k}{2}\}$, then $\varphi^i - 1 \in \Phi c_{\frac{k}{2}+i,2i}$. Consequently, $(A \setminus 2\Phi) \subseteq \mathcal{D}$ and $(A^{-1} \setminus 2^{-1}\Phi) \subseteq \mathcal{D}$. Furthermore, $2 \in \mathcal{D}$ if and only if $6 \mid k$. Hence, in this case, $(A \cup A^{-1}) \subseteq \mathcal{D}$.*

Also, we have the following analogues result on $A \cap \mathcal{D}$ from Lemma 4.8 provided that p is in $\mathcal{Q}_k \cup \mathcal{A}_k \cup \mathcal{B}_k$, where $\mathcal{B}_k$ is a finite set of primes depending on k which can be determined explicitly just like $\mathcal{Q}_k$ and $\mathcal{A}_k$.

Lemma 4.16. *Let k be odd. Then there exists a finite set of primes (depending on k) such that if p is not in this set, then $A \cap \mathcal{D} = \varnothing$.*

With Theorem 4.11(1), we can refine Theorem 3.11.

Corollary 4.17. *Let $p \notin \mathcal{Q}_k \cup \mathcal{A}_k$. If k is odd and $b \in F^*$, then*

$$2t_b + t_{b^{-1}} = \begin{cases} 2 & \text{if } b \in A, \\ 1 & \text{if } b \in A^{-1}, \\ 0 & \text{otherwise.} \end{cases}$$

Combining Theorem 4.11 and Lemma 4.13 we get

Corollary 4.18. *Let k be even and assume $p \notin \mathcal{Q}_k \cup \mathcal{A}_k$. Then $\{2, 2^{-1}\} \nsubseteq A \cap A^{-1}$.*

Proof. Since the coset containing

$$2 = (-1)((-1) - 1) = (-1)(\varphi^{\frac{k}{2}} - 1) \in \Phi(\varphi^{\frac{k}{2}} - 1) \subseteq A,$$

does not appear among the relevant cosets listed in Theorem 4.11. Thus, $2 \notin A \cap A^{-1}$, and so $2^{-1} \notin A \cap A^{-1}$ as well. $\square$

We have now characterized the intersection $A \cap A^{-1}$ both over $\mathbb{C}$ and in finite fields. The complex case reveals that this intersection is tightly constrained by cyclotomic identities, occurring only when k is divisible by 3 or 5. In the finite setting, these constraints persist except for a finite set of exceptional characteristics, captured by $\mathcal{A}_k$, and by $\mathcal{B}_k$ if applicable.

5. The case $x^m + by^m - bz^m = 1$, part II

Recall that when $\pm b \notin \Phi$, the counting formula for N_b takes the form

$$N_b = |S| + |T| = (k + s_b)m^3 + (2t_b + t_{b^{-1}})m^2 + m. \tag{22}$$

In this section, for even k, we determine the numerical quantities s_b and $2t_b + t_{b^{-1}}$. The results are consolidated in Table 1 and Theorems 1.3–1.4, with Theorem 1.5 completing the classification of the remaining cases. Their possible values have already been classified in broad terms: Theorems 3.3–3.6 describe the cases for s_b, and Theorems 3.13–3.14 give the corresponding distinctions for $2t_b + t_{b^{-1}}$. Section 4 provided the structural ingredients, with Lemma 4.4 showing how overlaps arise in $A \cup A^{-1}$. In the proofs that follow, the enumeration of s_b is guided by Theorem 3.6, the overlap classification, and Theorem 4.11 on $A \cap A^{-1}$, while the values of $2t_b + t_{b^{-1}}$ are established using Theorems 3.13 and 3.14.

5.1. Enumeration for $b \in A \cup A^{-1}$

For completeness, we recall here that the first row of Table 1, where $b \in \Phi(\varphi^{\frac{k}{6}} - 1) = \Phi$, falls into the boundary of the next subsection. It has already been treated in [12], with the result recorded as Theorem 1.1.

The following subsection covers the second and third rows of Table 1. In these cases, we will see that overlaps are not present.

5.1.1. $b \in 2\Phi \cup 2^{-1}\Phi$. We begin with the cases in the second and third rows of Table 1, namely when b lies in the exceptional cosets 2Φ or $2^{-1}\Phi$. These situations were excluded from Theorem 1.2, and their enumeration requires separate treatment. The formulas will depend on whether $6 \mid k$, as indicated in Table 1, and and the proofs draw on the preparatory results of Section 4.

Theorem 5.1. *Let (p, k) be a Ferrero pair with $p \notin \mathcal{Q}_k$. We have*

(1) *If $6 \nmid k$, then*
$$N_b = \begin{cases} km^3 + 2m^2 + m & \text{if } b \in 2\Phi, \\ km^3 + m^2 + m & \text{if } b \in 2^{-1}\Phi. \end{cases}$$

(2) *If $6 \mid k$, then*
$$N_b = \begin{cases} (k+2)m^3 + 2m^2 + m & \text{if } b \in 2\Phi, \\ (k+2)m^3 + m^2 + m & \text{if } b \in 2^{-1}\Phi. \end{cases}$$

Proof. By Corollary 4.18 we have $2 \in A \backslash A^{-1}$ and $2^{-1} \in A^{-1} \backslash A$. Therefore Theorem 3.13 gives the $2t_b + t_{b^{-1}} = 2$ if $b \in 2\Phi$ and $2t_b + t_{b^{-1}} = 1$ if $b \in 2^{-1}\Phi$, which account for the m^2 parts in both cases.

When $6 \nmid k$, Lemma 4.15 says that $2, 2^{-1} \notin \mathcal{D}$, and so $s_b = 0$. Putting this together with $2t_b + t_{b^{-1}}$ into (22), we have (1).

Assume that $6 \mid k$. By Lemma 4.1 we have $2, -2 \in \Phi c_{\frac{k}{6}, \frac{k}{2}}$ and $2^{-1}, -2^{-1} \in \Phi c_{\frac{k}{2}, \frac{k}{6}}$.

Suppose that $c_{\frac{k}{6}, \frac{k}{2}}$ is involved in a nontrivial overlap $o = (\frac{k}{6}, \frac{k}{2} \mid s, t)$. Since $\frac{k}{2}$ is involved, we know from (14) that o has to match one of $(\frac{k}{4}, \frac{k}{6} \mid \frac{k}{2}, \frac{k}{4})$ and $(\frac{k}{6}, \frac{k}{4} \mid \frac{k}{4}, \frac{k}{2})$ after applying some permutations listed in (8) and vice versa. However, no permutation in (8) can transform $\frac{k}{6}$ and $\frac{k}{2}$ of $(\frac{k}{4}, \frac{k}{6} \mid \frac{k}{2}, \frac{k}{4})$ or $(\frac{k}{6}, \frac{k}{4} \mid \frac{k}{4}, \frac{k}{2})$ into the same left-hand half, and so $c_{\frac{k}{6}, \frac{k}{2}}$ cannot be involved in a nontrivial overlap. Therefore, Theorem 3.5 yields $s_b = 2$. Again, this and $2t_b + t_{b^{-1}}$ together yield the result by (22). □

5.1.2. Enumeration for $b \in \Phi(\varphi^i - 1)$, $1 \le i < \frac{k}{2}$, and beyond. This subsection corresponds to the fourth row and onward of Table 1 together with Theorems 1.3. Now, elements b from $\Phi(\varphi^i - 1)$ $(1 \le i < \frac{k}{2})$ are naturally involved in overlaps. With this in mind, we proceed to their proofs.

When $6 \mid k$ the involved overlaps for $b \in \Phi(\varphi^i - 1)$ are nontrivial except for the special indices $i = \frac{k}{6}$ or $i = \frac{k}{3}$. For the trivial overlap cases, we just need to take care of the situation when $i = \frac{k}{3}$ as $i = \frac{k}{6}$ has been done in [12].

Theorem 5.2. *Let (p, k) be a Ferrero pair with $p \notin \mathcal{Q}_k$ and $6 \mid k$. We have*
$$N_b = \begin{cases} (k+4)m^3 + 4m^2 + m & \text{if } b \in \Phi(\varphi^{\frac{k}{3}} - 1), \\ (k+4)m^3 + 2m^2 + m & \text{if } b \in \Phi(\varphi^{\frac{k}{3}} - 1)^{-1}. \end{cases}$$

Proof. Again, write $k = 6\ell$. Let $b \in \Phi(\varphi^{\frac{k}{3}} - 1) = \Phi(\varphi^{2\ell} - 1) \subseteq A$. By Lemma 4.3, $b \notin \Phi$. Since $\Phi(\varphi^{\frac{k}{3}} - 1) \cap \Phi(\varphi^{\frac{k}{2}} - 1) = \varnothing$ by Lemma 2.8, we have $b \notin 2\Phi$.

Moreover, Theorem 4.11 together with Lemma 4.13 shows that $b \notin A^{-1}$. Thus, we have $2t_b + t_{b^{-1}} = 4$ by Theorem 3.14. As b and b^{-1} are not involved in any nontrivial overlap by Theorem 2.13, and $\frac{k}{3} \neq \frac{k}{2}$ we have $s_b = 4$ by Theorem 3.5. Now, the result follows from (22).

The case $b \in \Phi(\varphi^{\frac{k}{3}} - 1)^{-1} \subseteq A^{-1}$ can be handled exactly the same way. □

With the enumeration for the 4th and 5th rows of Table 1 now established, we are left to face the situation when b is involved in some nontrivial overlaps. Theorem 3.6 comes into play.

The first of the three cases in Theorem 3.6 is $b \in \Phi c_{\frac{k}{4},\frac{k}{2}} \cup \Phi c_{\frac{k}{2},\frac{k}{4}}$ with $12 \mid k$. Let us discuss it in some detail. So, we assume that $12 \mid k$ and write $k = 12\ell$. The only nontrivial overlaps containing $6\ell = \frac{k}{2}$ are the ones in (14), namely $(2\ell, 3\ell \mid 3\ell, 6\ell)$ and $(3\ell, 2\ell \mid 6\ell, 3\ell)$. Thus for

$$b \in \Phi c_{2\ell,3\ell} = \Phi c_{3\ell,6\ell} = \Phi c_{\frac{k}{4},\frac{k}{2}} \quad \text{or} \quad b \in \Phi c_{3\ell,2\ell} = \Phi c_{6\ell,3\ell} = \Phi c_{\frac{k}{2},\frac{k}{4}}, \tag{23}$$

we have $s_b = 6$ (and there are no other cases with $p \notin \mathcal{Q}_k$).

As φ^ℓ is a root of the 12th cyclotomic polynomial $x^4 - x^2 + 1$ we have

$$\begin{aligned} c_{3\ell,6\ell} &= \frac{\varphi^{6\ell}-1}{\varphi^{3\ell}-1} = \frac{-2}{\varphi^{3\ell}-1} \in \Phi\frac{2}{\varphi^{3\ell}-1}, \\ c_{2\ell,3\ell} &= \frac{\varphi^{3\ell}-1}{\varphi^{2\ell}-1} = \frac{\varphi^{3\ell}-1}{\varphi^{4\ell}} \in \Phi(\varphi^{3\ell}-1) \subseteq A. \end{aligned}$$

The coset $\Phi(\varphi^{3\ell} - 1)$ plays a central role in both the overlap structure and the block intersection count. By (23), we have

$$\Phi(\varphi^{\frac{k}{4}} - 1) = \Phi(\varphi^{3\ell} - 1) = \Phi c_{2\ell,3\ell} = \Phi c_{3\ell,6\ell} = \Phi\frac{2}{\varphi^{3\ell}-1} \subseteq A.$$

Similarly,

$$\Phi(\varphi^{\frac{k}{4}} - 1)^{-1} = \Phi(\varphi^{3\ell} - 1)^{-1} = \Phi c_{3\ell,2\ell} = \Phi c_{6\ell,3\ell} = \Phi\frac{\varphi^{3\ell}-1}{2} \subseteq A^{-1}.$$

Theorem 5.3. *Let (p,k) be a Ferrero pair with $12 \mid k$ and $p \notin \mathcal{Q}_k$. Then we have*

$$N_b = \begin{cases} (k+6)m^3 + 4m^2 + m & \text{if } b \in \Phi(\varphi^{\frac{k}{4}} - 1), \\ (k+6)m^3 + 2m^2 + m & \text{if } b \in \Phi(\varphi^{\frac{k}{4}} - 1)^{-1}. \end{cases}$$

Proof. In both cases, we have $s_b = 6$ by Theorem 3.6. Thus, with (22),

$$N_b = (k+6)m^3 + (2t_b + t_{b^{-1}})m^2 + m.$$

We are left with finding $2t_b + t_{b^{-1}}$.

If $b \in 2\Phi$, then $2\Phi = (\varphi^{3\ell}-1)\Phi$, and $\frac{2}{\varphi^{3\ell}-1} = -\frac{(-1)-1}{\varphi^{3\ell}-1} \in \Phi$. This contradicts Lemma 2.8. Therefore, $b \in A \setminus 2\Phi$. Theorem 4.11 with Lemma 4.13 implies $b \notin A^{-1}$. Now by Theorem 3.14, $2t_b + t_{b^{-1}} = 4$ if $b \in \Phi(\varphi^{3\ell} - 1) = \Phi c_{2\ell,3\ell}$, and $2t_b + t_{b^{-1}} = 2$ if $b \in \Phi(\varphi^{3\ell} - 1)^{-1} = \Phi c_{3\ell,2\ell}$. □

Another instance for $12 \mid k$ occurs when $b \in A \cap A^{-1}$, as stated in Theorem 4.11(4) (as well as in Theorem 4.6(4)). In this case, with a 12th root of unity ρ in Φ, we have $\Phi(\sigma - 1) \cup \Phi(\sigma^5 - 1) = A \cap A^{-1}$.

Theorem 5.4. *Let (p, k) be a Ferrero pair with $p \notin \mathcal{Q}_k$ and $12 \mid k$. Then for b in the union of cosets $\Phi(\varphi^{\frac{k}{12}} - 1) \cup \Phi(\varphi^{\frac{5k}{12}} - 1)$ we have*

$$N_b = (k+8)m^3 + 6m^2 + m.$$

Proof. By Theorem 4.6(4) we have $b \in (A \cap A^{-1}) \setminus (2\Phi \cup 2^{-1}\Phi)$, thus by Theorem 3.14 $2t_b + t_{b^{-1}} = 6$. Lemma 4.4 gives that b is involved in a nontrivial overlap, but not in a triple overlap by Theorem 2.13. Thus Theorem 3.6 implies $s_b = 8$. Now (22) yields the result. □

Having completed the enumeration for the $12 \mid k$ cases, we now move to the second of the three cases in Theorem 3.6 for those b that are involved in triple overlaps. These are precisely the cosets listed in the remaining rows of Table 1 under the condition $30 \mid k$ as we shall see next.

Suppose that $b \in \Phi c_{j,i}$ and is involved in a nontrivial triple overlap. By Theorem 2.13 we have $k = 30\ell$, $\ell \in \mathbb{N}$. Thus there exists $\tau \in \Phi$ of order 30. Then τ^5 is a primitive 6th root of unity, hence $\tau^{10} - \tau^5 + 1 = 0$.

Notice that each nontrivial triple overlap involves $c_{5\ell,u\ell}$ or $c_{u\ell,5\ell}$ for some u (see Theorem 2.13). Therefore, we find that b or b^{-1} is contained in

$$\Phi c_{5\ell,u\ell} = \Phi\frac{\tau^u - 1}{\tau^5 - 1} = \Phi\frac{\tau^u - 1}{\tau^{10}} = \Phi(\tau^u - 1) \subseteq A. \tag{24}$$

Also, we have

$$\Phi(\tau^u + 1) = \Phi(-\tau^{15+u} + 1) = \Phi(\tau^{15+u} - 1) \subseteq A. \tag{25}$$

These identities will be used freely in what follows.

We first do the triple overlap $(3\ell, 5\ell \mid 5\ell, 9\ell \mid 6\ell, 12\ell)$. In this case, we have $b \in \Phi c_{\frac{k}{6},\frac{k}{10}} = \Phi c_{\frac{3k}{10},\frac{k}{6}} = \Phi c_{\frac{2k}{5},\frac{k}{5}} \subseteq A \cap A^{-1}$ by Theorem 4.6. Here we note that $b^{-1} \in \Phi(\tau^9 - 1)$, and by Lemma 2.8, b and b^{-1} are from different cosets.

Theorem 5.5. *Let (p, k) be a Ferrero pair with $p \notin \mathcal{Q}_k$ and $30 \mid k$. Let $\tau = \varphi^{\frac{k}{30}} \in \Phi$, which is of order 30. For $b \in \Phi(\tau^3 - 1)$ we have*

$$N_b = N_{b^{-1}} = (k+12)m^3 + 6m^2 + m.$$

Proof. Write $k = 30\ell$, as before. As $b \in A \cap A^{-1}$, Theorem 3.14 shows $2t_b + t_{b^{-1}} = 6$. Also, as $c_{5\ell,3\ell}$ is involved in a triple overlap, $s_b = 12$ by Theorem 3.6. Putting this into (22), we obtain the result.

For b^{-1} the same arguments apply to give the same result. □

We are now going for the remaining nontrivial triple overlaps. By Theorem 2.13 these are

$$(\ \ell, 2\ell \mid 4\ell, 9\ell \mid 5\ell, 14\ell), \quad (4\ell, 5\ell \mid 8\ell, 11\ell \mid 9\ell, 14\ell),$$
$$(2\ell, 3\ell \mid 5\ell, 8\ell \mid 7\ell, 14\ell), \quad (2\ell, 5\ell \mid 3\ell,\ 8\ell \mid 4\ell, 13\ell).$$

In each case we have $b \in A \cup A^{-1}$ (and so $b^{-1} \in A \cup A^{-1}$ as well). For example, the first triple overlap contains the constituent $(\ell, 2\ell \mid 5\ell, 14\ell)$. This is equivalent to $(5\ell, 14\ell \mid \ell, 2\ell)$ by applying the permutation $(s_1, s_2)(t_1, t_2)$ (cf. (8)). Another application of the permutation (s_1, t_2), we get $(5\ell, \ell \mid 14\ell, 2\ell) = (\frac{k}{2}, i \mid \frac{k}{2} - i, 2i)$ with $i = \frac{k}{30}$. Thus, we see from Theorem 4.4 that if b is involved in the first triple overlap, then it is from $\Phi(\varphi^i - 1) \subseteq A$.

Theorem 5.6. *Let (p, k) be a Ferrero pair with $p \notin \mathcal{Q}_k$ and $30 \mid k$. Let $\tau \in \Phi$ have order 30. For*

$$b \in \Phi(\tau^2 - 1) \cup \Phi(\tau^4 - 1) \cup \Phi(\tau^8 - 1) \cup \Phi(\tau^{14} - 1),$$

we have

$$N_b = (k + 12)m^3 + 4m^2 + m,$$
$$N_{b^{-1}} = (k + 12)m^3 + 2m^2 + m.$$

Proof. In all cases $b \in A$. Moreover, from the preceding remark, we find that b and b^{-1} are involved in a nontrivial triple overlap. Theorem 4.11 gives $b \in A \setminus A^{-1}$, and thus $b^{-1} \in A^{-1} \setminus A$.

Now, Theorems 3.14, and 3.6 together with (22) give the result. □

With the triple overlap cases resolved, all rows of Table 1 have now been accounted for: $b \in \Phi$, $2\Phi \cup 2^{-1}\Phi$, $\Phi(\varphi^{\frac{k}{3}} - 1) \cup \Phi(\varphi^{\frac{k}{3}} - 1)^{-1}$, $\Phi(\varphi^{\frac{k}{4}} - 1) \cup \Phi(\varphi^{\frac{k}{4}} - 1)^{-1}$, and $A \cap A^{-1}$. What remains is the generic situation, where $b \in A \cup A^{-1}$but no triple overlaps occur and all previously discussed special cases are excluded. This is precisely the setting of Theorem 1.3, which we now prove.

Proof of Theorem 1.3. As b is inside $A \cup A^{-1}$, but not in $A \cap A^{-1}$ and no other special cases present, there is a nontrivial overlap by Lemma 4.4, but no triple overlap. Thus $s_b = 8$ by Theorem 3.6. The numbers for $2t_b + t_{b^{-1}}$ come from Theorem 3.14. □

This completes the proof of Theorem 1.3. Together with the special cases and triple overlaps already resolved, we now have a full enumeration of the solution counts for all cases with $b \in A \cup A^{-1}$. In the next subsection, we turn to Theorem 1.4, which addresses the remaining situation.

5.2. *Enumeration for $b \in \mathcal{D} \setminus (A \cup A^{-1})$*

This subsection addresses the situation outside $A \cup A^{-1}$. The enumeration is given by Theorem 1.4. For the remaining cases, namely when $3 \nmid k$, the enumeration is provided by Theorem 1.5. Together, these two results complete the classification for all $b \in \mathcal{D} \setminus (A \cup A^{-1})$ when k is even.

First, we prove Theorem 1.4.

Proof of Theorem 1.4. As $2\Phi \subseteq A$ and likewise $2^{-1}\Phi \subseteq A^{-1}$, Theorem 3.14 applies to give $2t_b + t_{b^{-1}} = 0$. It remains to determine s_b. The first two statements are direct from Theorem 3.5 with $s_b = 2$ and 4, respectively. For the third case, we assume that $b \in \Phi c_{i,j}$ is involved in a nontrivial overlap and $\frac{k}{2} \notin \{i, j\}$. In this case, $6 \mid k$ by Theorem 2.13. If b

is involved in a nontrivial triple overlaps, then $b \in A \cap A^{-1}$ as we have seen in the previous subsection (explicitly, Theorems 5.5 and 5.6 and the discussions). Since we have assumed that $b \notin A \cup A^{-1}$, we see that b cannot be involved in any nontrivial triple overlap. By Theorem 3.6, we have $s_b = 8$. □

Remark 5.7. (1) Here is a list of the relevant overlap cases in the preceding theorem:

- $42 \mid k$: all of $\mathcal{O}_{42}$.
- $60 \mid k$: all of $\mathcal{O}_{60}$, with all variations.
- $k = 30\ell_1$ (see $\mathcal{O}_{30}$):

$$\begin{aligned}&(\ \ell_1, 3\ell_1 \mid 3\ell_1, 11\ell_1),\ \ (7\ell_1, 9\ell_1 \mid 9\ell_1, 13\ell_1),\ \ (\ell_1, 4\ell_1 \mid 2\ell_1, 9\ell_1),\\ &(2\ell_1, 7\ell_1 \mid 3\ell_1, 14\ell_1),\ \ (3\ell_1, 4\ell_1 \mid 8\ell_1, 13\ell_1),\end{aligned}$$

  with only the inverses as variations.

(2) When $6 \mid k$, $b \notin A \cup A^{-1}$ is equivalent to requiring $i \neq \frac{k}{6}$, $j \neq \frac{k}{6}$, and $i \neq 2j$, $j \neq 2i$. For example, if b is in $\Phi c_{\ell_1, 4\ell_1}$ or $\Phi c^{-1}_{\ell_1, 4\ell_1}$, then $b \notin A \cup A^{-1}$. However, $c_{\ell_1, 2\ell_1} = \varphi^{\ell_1} + 1 = (-1)(\varphi^{\frac{k}{2}+\ell_1} - 1) \in A$.

Finally, for the remaining cases when $3 \nmid k$, the enumeration is given by Theorem 1.5. Since the cubic term is already determined in Theorem 3.5 and the quadratic coefficient α has been fixed in Theorems 3.13 and 3.14, no further proof is required here.

With all cases now resolved, the enumeration of solutions to equation

$$x^m + by^m - bz^m = 0,$$

is complete for Ferrero pairs (p, k) with even k and $p \notin \mathcal{Q}_k$. Each instance of $b \in F^*$ has been accounted for, and the corresponding value of N_b determined. Together with Theorems 1.6 and 1.7 announced in the introduction, which settle the odd-k cases subject to the exclusion of the finite sets of exceptional primes $\mathcal{Q}_k$ and $\mathcal{A}_k$, the enumeration of N_b is complete for all values of k.

5.3. Algorithms and examples for the enumeration of N_b

We systematize the enumeration of N_b by separating the analysis according to the parity of k and, in the even case, the divisibility by 3. This yields three distinct procedures: Algorithm 1 applies when k is even with $3 \nmid k$; Algorithm 2 applies when k is even with $3 \mid k$; Algorithm 3 applies when k is odd. Each algorithm is accompanied by an example or two worked out in the finite field $F = \mathrm{GF}(q)$ with $q = 83^2 = 6889$. For this q, we have $8 \mid (q-1)$, $12 \mid (q-1)$, and $7 \mid (q-1)$, and in each case the prime p lies outside the excluded sets: $p \notin \mathcal{Q}_8$, $p \notin \mathcal{Q}_{12}$, and $p \notin \mathcal{Q}_7 \cup \mathcal{A}_7$. The worked examples show how the branching criteria lead to termination in different cases. Let ζ be a primitive element of F.

The first algorithm applies when k is even with $3 \nmid k$. The pseudocode is given in Algorithm 1.

Algorithm 1 Enumeration of N_b for even k with $3 \nmid k$

```
Input: q, k (even, 3∤k), m = (q−1)/k, b ∈ F_q^* \ Φ
IF b ∈ 2Φ ∪ 2^{-1}Φ THEN // Theorem 5.1(1)
```

$$N_b = \begin{cases} km^3 + 2m^2 + m & \texttt{if } b \in 2\Phi \\ km^3 + m^2 + m & \texttt{if } b \in 2^{-1}\Phi \end{cases}$$

```
ELSE IF b ∈ Φc_{i,j} THEN // Theorem 1.5
```

$$N_b = \begin{cases} (k+2)m^3 + \alpha m^2 + m & \texttt{if } i = \frac{k}{2} \texttt{ or } j = \frac{k}{2} \\ (k+4)m^3 + \alpha m^2 + m & \texttt{otherwise} \end{cases}$$

```
    CASE: // Theorem 3.14 gives α = 2t_b + t_{b−1}
```

$$\alpha = \begin{cases} 6 & \texttt{if } b \in A \cap A^{-1} \\ 4 & \texttt{if } b \in A \setminus A^{-1} \\ 2 & \texttt{if } b \in A^{-1} \setminus A \\ 0 & \texttt{if } b \notin A \cup A^{-1} \end{cases}$$

```
    ENDCASE
ELSE // Theorem 1.2
```

$$N_b = km^3 + m$$

```
ENDIF
```

We illustrate the algorithm for $k = 8$ by computing N_b for $b = \zeta^{100}$ in $F^* \setminus \Phi$, $\Phi = \langle \zeta^m \rangle$ with $m = 861$. We have

$$\Phi = \{\zeta^{861}, \zeta^{1722}, \zeta^{2583}, \zeta^{3444}, \zeta^{4305}, \zeta^{5166}, \zeta^{6027}, 1\}.$$

According to Algorithm 1, we first check if $b \in 2\Phi$ or $2^{-1}\Phi$. Since $2 = \zeta^{84}$, we have $2b = \zeta^{184} \notin \Phi$ and $2^{-1}b = \zeta^{16} \notin \Phi$; hence $b \notin 2\Phi \cup 2^{-1}\Phi$. Next, to determine if $b \in \mathcal{D}$, we arrange the representatives $c_{i,j}$ in a $\frac{k}{2} \times \frac{k}{2}$ matrix $\overline{D}$, which allows each coset $\Phi c_{i,j}$ to be recognized by its (i,j) position:

$$\overline{D} = \begin{pmatrix} \zeta^0 & \zeta^{3137} & \zeta^{6232} & \zeta^{4040} \\ \zeta^{3751} & \zeta^0 & \zeta^{3095} & \zeta^{903} \\ \zeta^{656} & \zeta^{3793} & \zeta^0 & \zeta^{4696} \\ \zeta^{2848} & \zeta^{5985} & \zeta^{2192} & \zeta^0 \end{pmatrix}.$$

Note that $b \in \Phi c_{i,j}$ if and only if $b^{-1}c_{i,j} \in \Phi$. We compute $b^{-1}\overline{D} = (c'_{i,j})$ with each $c'_{i,j} = b^{-1}c_{i,j}$:

$$b^{-1}\overline{D} = \begin{pmatrix} \zeta^{6788} & \zeta^{3037} & \zeta^{6132} & \zeta^{3940} \\ \zeta^{3651} & \zeta^{6788} & \zeta^{2995} & \zeta^{803} \\ \zeta^{556} & \zeta^{3693} & \zeta^{6788} & \zeta^{4596} \\ \zeta^{2748} & \zeta^{5885} & \zeta^{2092} & \zeta^{6788} \end{pmatrix}.$$

Algorithm 2 Enumeration of N_b for even k with $3 \mid k$

Input: q, k (even, $3\mid k$), $m=(q-1)/k$, $b\in F_q^*\setminus\Phi$

IF $b\in A\cup A^{-1}$ THEN // Table 1

IF b matches a row of Table 1 THEN

$N_b=$ the value given in the corresponding row

ELSE // Theorem 1.3

$$N_b=\begin{cases}(k+8)m^3+4m^2+m & \text{if } b\in A\setminus A^{-1}\\ (k+8)m^3+2m^2+m & \text{if } b\in A^{-1}\setminus A\end{cases}$$

ENDIF

ELSE IF $b\in \Phi c_{i,j}$ THEN // Theorem 1.4

$$N_b=\begin{cases}(k+2)m^3+m & \text{if } i=\frac{k}{2} \text{ or } j=\frac{k}{2}\\ (k+4)m^3+m & \text{if } \frac{k}{2}\notin\{i,j\}, \text{ and w/o nontrivial overlap}\\ (k+8)m^3+m & \text{if } \frac{k}{2}\notin\{i,j\}, \text{ and w/ nontrivial overlap}\end{cases}$$

ELSE // Theorem 1.2

$N_b=km^3+m.$

ENDIF

Since none of the entries of $b^{-1}\overline{D}$ belong to Φ, we conclude that $b\notin\mathcal{D}$. Therefore, b falls into the final branch of Algorithm 1, and we obtain

$$N_b=km^3+m=8\cdot 861^3+861=5,106,219,909.$$

The second algorithm applies when k is even with $3\mid k$. The pseudocode is given in Algorithm 2.

The smallest even integer to which Algorithm 2 applies is $k=6$. In this case, we have

$$A=\Phi(\varphi-1)\cup\Phi(\varphi^2-1)\cup\Phi(\varphi^3-1)=\Phi(\varphi^{\frac{k}{6}}-1)\cup\Phi(\varphi^{\frac{k}{3}}-1)\cup\Phi(\varphi^{\frac{k}{2}}-1).$$

Thus, if $b\in A\cup A^{-1}$, then b matches one of the first five rows of Table 1. By Theorem 2.13, however, b is not involved in any nontrivial overlap. Consequently, when $b\notin A\cup A^{-1}$, for $b\in\Phi c_{i,j}$, we have $N_b=(k+2)m^3+m$ or $(k+4)m^3+m$ depending on whether $\frac{k}{2}\in\{i,j\}$ or not, and for all other b, $N_b=km^3+m$.

The first true overlap situation arises at k=12 when overlaps enter Algorithm 2 in a substantive way. Let us illustrate the algorithm for $k=12$ by computing N_b for $b=\zeta^{245}$ and $b=\zeta^{504}$ in $F^*\setminus\Phi$, $\Phi=\langle\zeta^m\rangle$ with $m=574$. We have

$$\Phi=\{\zeta^{574},\zeta^{1148},\zeta^{1722},\zeta^{2296},\zeta^{2870},\zeta^{3444},\zeta^{4018},\zeta^{4592},\zeta^{5166},\zeta^{5740},\zeta^{6314},1\}.$$

First, consider $b=\zeta^{245}$. According to Algorithm 2, we first check if $b\in A\cup A^{-1}$. Notice that $b\in A\cup A^{-1}$ if and only if $b^{-1}(A\cup A^{-1})\cap\Phi\neq\varnothing$. Thus, we arrange the representatives φ^i-1 and $(\varphi^i-1)^{-1}$ in a matrix $\overline{A}$, which allows each coset $\Phi(\varphi^i-1)$ and $\Phi(\varphi^i-1)^{-1}$

to be recognized by its $(1, i)$ and $(2, i)$ position:

$$\overline{A} = \begin{pmatrix} \zeta^{6167} & \zeta^{2296} & \zeta^{2625} & \zeta^{5894} & \zeta^{5887} & \zeta^{3528} \\ \zeta^{721} & \zeta^{4592} & \zeta^{4263} & \zeta^{994} & \zeta^{1001} & \zeta^{3360} \end{pmatrix}.$$

Now, multiplying by b^{-1}, we get

$$b^{-1}\overline{A} = \begin{pmatrix} \zeta^{5922} & \zeta^{2051} & \zeta^{2380} & \zeta^{5649} & \zeta^{5642} & \zeta^{3283} \\ \zeta^{476} & \zeta^{4347} & \zeta^{4018} & \zeta^{749} & \zeta^{756} & \zeta^{3115} \end{pmatrix}.$$

Since $b^{-1}(\varphi^3 - 1)^{-1} = \zeta^{4018} \in \Phi$, it follows that $b \in \Phi(\varphi^3 - 1)^{-1} = \Phi(\varphi^{\frac{k}{4}} - 1)^{-1}$. Thus Algorithm 2 terminates in the first branch, matching the second row of $12 \mid k$ cases. We thus have

$$N_b = (k + 6)m^3 + 2m^2 + m = 18 \cdot 574^3 + 2 \cdot 574^2 + 574 = 3,404,805,558.$$

Next, consider $b = \zeta^{504}$. We have

$$b^{-1}\overline{A} = \begin{pmatrix} \zeta^{5663} & \zeta^{1792} & \zeta^{2121} & \zeta^{5390} & \zeta^{5383} & \zeta^{3024} \\ \zeta^{217} & \zeta^{4088} & \zeta^{3759} & \zeta^{490} & \zeta^{497} & \zeta^{2856} \end{pmatrix},$$

which has nothing common with Φ and so $b \notin A \cup A^{-1}$. According to Algorithm 2, we next check whether $b \in \mathcal{D}$. As explained in the example for Algorithm 1, this is done by comparing $b^{-1}\mathcal{D}$ with Φ. Thus, we arrange $c_{i,j}$'s in the matrix $\overline{D}$ and compute

$$b^{-1}\overline{D} = \begin{pmatrix} \zeta^{6384} & \zeta^{2513} & \zeta^{2842} & \zeta^{6111} & \zeta^{6104} & \zeta^{3745} \\ \zeta^{3367} & \zeta^{6384} & \zeta^{6713} & \zeta^{3094} & \zeta^{3087} & \zeta^{728} \\ \zeta^{3038} & \zeta^{6055} & \zeta^{6384} & \zeta^{2765} & \zeta^{2758} & \zeta^{399} \\ \zeta^{6657} & \zeta^{2786} & \zeta^{3115} & \zeta^{6384} & \zeta^{6377} & \zeta^{4018} \\ \zeta^{6664} & \zeta^{2793} & \zeta^{3122} & \zeta^{6391} & \zeta^{6384} & \zeta^{4025} \\ \zeta^{2135} & \zeta^{5152} & \zeta^{5481} & \zeta^{1862} & \zeta^{1855} & \zeta^{6384} \end{pmatrix}.$$

We find $b^{-1}c_{4,6} = \zeta^{4018} \in \Phi$. Therefore, $b \in \Phi c_{4,6} = \Phi c_{\frac{k}{3},\frac{k}{2}}$, and Algorithm 2 terminates in the second branch. Matching up Theorem 1.4, we obtain

$$N_b = (k + 2)m^3 + m = 18 \cdot 574^3 + 574 = 3,404,146,606.$$

The third algorithm applies when k is odd. The pseudocode is given in Algorithm 3.

We illustrate the algorithm for $k = 7$ by computing N_b for $b = \zeta^{492}$ in $F^* \setminus \Phi$, $\Phi = \langle \zeta^m \rangle$ with $m = 984$. We have

$$\Phi = \{\zeta^{984}, \zeta^{1968}, \zeta^{2952}, \zeta^{3936}, \zeta^{4920}, \zeta^{5904}, 1\}.$$

According to Algorithm 3, we first check whether $b \in \mathcal{D}$ or not. To do this, the matrix $\overline{D}$ with entries $c_{i,j}$ is used, and $b^{-1}\overline{D}$ is computed:

$$b^{-1}\overline{D} = \begin{pmatrix} \zeta^{6396} & \zeta^{4872} & \zeta^{1584} & \zeta^{2076} & \zeta^{6348} & \zeta^{1968} \\ \zeta^{1032} & \zeta^{6396} & \zeta^{3108} & \zeta^{3600} & \zeta^{984} & \zeta^{3492} \\ \zeta^{4320} & \zeta^{2796} & \zeta^{6396} & \zeta^{0} & \zeta^{4272} & \zeta^{6780} \\ \zeta^{3828} & \zeta^{2304} & \zeta^{5904} & \zeta^{6396} & \zeta^{3780} & \zeta^{6288} \\ \zeta^{6444} & \zeta^{4920} & \zeta^{1632} & \zeta^{2124} & \zeta^{6396} & \zeta^{2016} \\ \zeta^{3936} & \zeta^{2412} & \zeta^{6012} & \zeta^{6504} & \zeta^{3888} & \zeta^{6396} \end{pmatrix}.$$

Algorithm 3 Enumeration of N_b for odd k

```
Input: q, k (odd), m = (q-1)/k, b ∈ F_q^* \ Φ

IF b ∈ D THEN // Theorem 1.7

    IF p = 2 THEN // Theorem 1.7(3)
```

$$N_b = \begin{cases} (k+4)m^3 + 2m^2 + m & \texttt{if } b \in A \\ (k+4)m^3 + m^2 + m & \texttt{if } b \in A^{-1} \\ (k+4)m^3 + m & \texttt{if } b \notin A \cup A^{-1} \end{cases}$$

```
    ELSE IF -b ∈ Φ THEN // // Theorem 1.7(2)
```

$$N_b = \begin{cases} (k+2)m^3 + 2m^2 + 2m & \texttt{if } b \in A \\ (k+2)m^3 + m^2 + 2m & \texttt{if } b \in A^{-1} \\ (k+2)m^3 + 2m & \texttt{if } b \notin A \cup A^{-1} \end{cases}$$

```
    ELSE // // Theorem 1.7(1)
```

$$N_b = \begin{cases} (k+2)m^3 + 2m^2 + m & \texttt{if } b \in A \\ (k+2)m^3 + m^2 + m & \texttt{if } b \in A^{-1} \\ (k+2)m^3 + m & \texttt{if } b \notin A \cup A^{-1} \end{cases}$$

```
    ENDIF

ELSE // Theorem 1.6
```

$$N_b = \begin{cases} km^3 + 2m^2 + m & \texttt{if } b \in A \\ km^3 + m^2 + m & \texttt{if } b \in A^{-1} \\ km^3 + m & \texttt{if } b \notin A \cup A^{-1} \end{cases}$$

```
ENDIF
```

From this, we see that $b = c_{3,4} \in \mathcal{D}$. As $p \neq 2$, Algorithm 3 indicates that we need to check if $-b = \zeta^{3936}$ is in Φ or not, which is the case. This leads us to check whether $b \in A$, $b \in A^{-1}$, or neither. Thus, we compute $b^{-1}\overline{A}$ where $\overline{A}$ is the matrix with entries $\varphi^i - 1$ and $(\varphi^i - 1)^{-1}$:

$$b^{-1}\overline{A} = \begin{pmatrix} \zeta^{5586} & \zeta^{4062} & \zeta^{774} & \zeta^{1266} & \zeta^{5538} & \zeta^{1158} \\ \zeta^{318} & \zeta^{1842} & \zeta^{5130} & \zeta^{4638} & \zeta^{366} & \zeta^{4746} \end{pmatrix}.$$

Since no entry of $b^{-1}\overline{A}$ is in Φ, $b \notin A \cup A^{-1}$, Algorithm 3 terminates in the third branch of the first branch. By Theorem 1.7(2), we obtain

$$N_b = (k+2)m^3 + 2m = 9 \cdot 984^3 + 2 \cdot 984 = 8,574,877,104.$$

6. The general case $ax^m + by^m - cz^m = 1$

We now turn to the general equation

$$ax^m + by^m - cz^m = 1, \tag{26}$$

for $a, b, c \in F^*$, where $F = \mathrm{GF}(q)$ with a primitive element ζ, q a prime power, $m \mid (q-1)$, and $\Phi = \langle \varphi \rangle$ with $\varphi = \zeta^m$. Denote by N the number of solutions of (26) over F. We do not impose the circularity condition, but will highlight when notable phenomena arise.

Recall that $\mathcal{D} = \cup\{\Phi(\varphi^j - 1)^{-1}(\varphi^i - 1) \mid i, j \in \boldsymbol{k}\} = -\mathcal{D}$, and for $r \in F^*$, $E_r = \{\Phi + \varphi^i r \mid i \in \boldsymbol{k}_0\}$. Set $\cup E_r = \cup_{i=0}^{k-1}(\Phi + \varphi^i r)$. These constructions allow us to describe precisely when intersections of Φ-blocks contribute to the solution count.

Theorem 6.1. *Let $u, v \in F^*$. Then*

(1) *$\Phi \cap (\Phi u + v) \neq \varnothing$ if and only if $v \in \Phi - \varphi^j u$ for some $j \in \mathbf{k}_0$, i.e. $v \in E_{-u}$.*

(2) *Suppose $\Phi \cap (\Phi u + v) \neq \varnothing$ and $v \in \Phi - \varphi^j u$ for some $j \in \mathbf{k}_0$. Then $|\Phi \cap (\Phi u + v)| = \ell \geq 1$ if and only if $v \in \Phi - \varphi^{j_i} u$ for exactly ℓ values $j_i \in \mathbf{k}_0$. In the case $\ell \geq 2$, both $u, v \in \mathcal{D}$.*

Proof. (1) We have

$$v \in \Phi - \varphi^j u \in E_{-u} \iff v = \varphi^i - \varphi^j u \iff \varphi^i = \varphi^j u + v \in \Phi \cap (\Phi u + v) \neq \varnothing.$$

(2) The first part is a straightforward consequence of (1). Suppose that $\ell \geq 2$. This means that $v \in (\Phi - \varphi^{j_1} u) \cap (\Phi - \varphi^{j_2} u)$ for some $j_1 \neq j_2$. Hence, $v = \lambda_1 - \varphi^{j_1} u = \lambda_2 - \varphi^{j_2} u$ for some distinct $\lambda_1, \lambda_2 \in \Phi$, and so $u = \frac{\varphi^{j_2} - \varphi^{j_1}}{\lambda_2 - \lambda_1} = \lambda_1^{-1} \varphi^{j_1} \frac{\varphi^{j_2 - j_1} - 1}{\lambda_1^{-1}\lambda_2 - 1} \in \mathcal{D}$. Also, if $\lambda, \mu \in \Phi$ such that $\lambda = \mu u + v \in \Phi \cap (\Phi u + v)$, then $\mu^{-1}\lambda = u + \mu^{-1} v \in \Phi \cap (\Phi v + u)$. Consequently, $|\Phi \cap (\Phi u + v)| = |\Phi \cap (\Phi v + u)|$. Therefore, $-v \in \mathcal{D}$, and so $v \in -\mathcal{D} = \mathcal{D}$ as well. □

Corollary 6.2. *Assume (F, Φ) is circular and $u, v \in F$. If $v \in \cup E_{-u}$, then v is contained in at most two blocks from E_{-u}, and containment in two blocks occurs precisely when $u \in \mathcal{D}$ and $v \in \mathcal{D}$.*

Proof. Suppose that v is contained in more than two blocks from E_{-u}. Then $\Phi \cap (\Phi u + v)$ contains more then two elements by the first part of Theorem 6.1(2). From the circularity we infer that $\Phi = \Phi u + v$. By [1, Proposition 5.4], it follows that $v = 0$ and $\Phi = \Phi u$. Since this is not the case, v is contained in at most two blocks from E_{-u}. The second part follows from the second part of Theorem 6.1(2). □

Theorem 6.1 describes the precise conditions under which intersections of cosets contribute to the solution set of (26). To translate these structural facts into explicit counts, we employ an algorithm, whose pseudocode is presented in Algorithm 4.

This algorithm decomposes the enumeration into three stages. First, it checks whether the equation reduces to a previously solved form. Second, it accounts for solutions with zeros in one coordinate. Third, it analyzes solutions with all coordinates nonzero. The following subsections detail these stages.

6.A. Checking for reduction possibility

First we check whether the Eq. (26) reduces to one of the previously settled forms. If $a \in \Phi$ and simultaneously $bc^{-1} \in \Phi$, then $a\Phi = \Phi$ and $b\Phi = c\Phi$, which make (26) "equivalent" to

$$x^m + by^m - bz^m = 1,$$

Algorithm 4 Enumeration of N in the general case

```
Input:

    q (prime power), m | (q − 1), a, b, c ∈ F = GF(q)
    Set k = (q − 1)/m, p = char(F), ζ a primitive element of F

Algorithm:
  1. Construct Φ = ⟨φ⟩, φ = ζ^m
  2. Check membership and eligibility
     • If k is large, go to Step 3
     • Check membership conditions:  a ∈ Φ and bc^{-1} ∈ Φ, or b ∈ Φ and ac^{-1}
        - If membership fails, proceed to Step 3
        - If membership holds, check prime eligibility
          ∗ If p ∈ Q_k and p ∈ A_k (when k is odd), proceed to Step 3
          ∗ Otherwise, apply Algorithms 1--3 to get N
  3. Compute n_0 = |Φ ∩ {a, b, −c}|
     • Contribute n_0 · m
  4. Compute t_x = |Φ ∩ (Φb − c)|, t_y = |Φ ∩ (Φa − c)|, t_z = |Φ ∩ (Φa + b)|
     • Set t = t_x + t_y + t_z
     • Contribute t · m^2
  5. Compute s = ∑_{λ∈Φ} |(Φa + λ(−c)) ∩ (1 − Φb))|
     • Contribute s · m^3

Output:

    Number N of solutions of ax^m + by^m − cz^m = 1 in F
    N = s · m^3 + t · m^2 + n_0 · m
```

in the sense that there is a one-one corresponding between the solution sets of both equations. Similarly, if $ac^{-1} \in \Phi$ and $b\Phi = \Phi$, then (26) is equivalent to

$$x^m + ay^m - az^m = 1.$$

In such cases, Algorithms 1–3 apply directly provided that $p = \mathrm{char}F$ is not in $\mathcal{Q}_k$ or $\mathcal{Q}_k \cup \mathcal{A}_k$ when k is odd. Recall that $A_k \subseteq Q_k$ if $6 \mid k$ or $10 \mid k$. This is not true in general (cf. Table 2). When k is large, one simply skips the prime-eligibility test and proceeds with Algorithm 4 as computing $\mathcal{Q}_k$ and $\mathcal{A}_k$ may be not feasible. Thus, failure of the membership conditions, failure of prime eligibility, or the case of large k all lead into the general intersection analysis.

We note that prime eligibility ($p \notin \mathcal{Q}_k$ or $p \notin \mathcal{Q}_k \cup \mathcal{A}_k$ when k odd) is only relevant when (26) reduces to one of the canonical forms. If reduction succeeds, as in Example 6.3, prime eligibility determines whether Algorithms 1–3 can be applied. If reduction fails, then prime eligibility has no effect, and Algorithm 4 must be used. In such cases, the general intersection analysis may even yield zero solutions, as illustrated in Example 6.4.

6.B. Solutions with zeros involved

The equation $ax^m = 1$ ($by^m = 1$ and $-cz^m = 1$, respectively) has solutions if and only if $a \in \Phi$ ($b \in \Phi$ and $-c \in \Phi$, respectively), and, in this case the number of solutions $x \in F^*$ ($y \in F^*$ and $z \in F^*$, respectively), will be m (see also Lemma 3.7).

Next, the equation $ax^m + by^m = 1$ has nontrivial solutions $x, y \in F^*$ if and only if $\Phi \cap (\Phi a + b) \neq \varnothing$. By Theorem 6.1, this occurs exactly when $b \in E_{-a}$, and that $|\Phi \cap (\Phi a + b)| \geq 2$ if and only if $a, b \in \mathcal{D}$. Each of the intersection points contributes m^2 solutions from $F^* \times F^* \times \{0\}$ to the equation.

The equations $ax^m - cz^m = 1$ and $by^m - cz^m = 1$ can be treated in a similar way.

6.C. Solutions with no zeros involved

Suppose that $(x, y, z) \in (F^*)^3$ is a solution to the equation. Put $e = 1 - by^m \in 1 - \Phi b$. Then $ax^m = cz^m + e \in \Phi a \cap (\Phi c + e)$. If $e = 0$, then $b \in \Phi$. In this case, $\Phi a = \Phi c$, and (26) is equivalent to $ax^m + y^m - az^m = 1$. Thus, failure of the membership conditions necessarily implies either $e \neq 0$ or $p = \mathrm{char} F$ lies in $\mathcal{Q}_k$ or $\mathcal{A}_k$ when k is odd. In this situation we proceed with the general intersection analysis.

From $\Phi a \cap (\Phi c + e) = a \cdot (\Phi \cap (\Phi a^{-1}c + a^{-1}e))$, we see that $a^{-1}e \in \cup E_{-a^{-1}c}$ when the intersection is nonempty, and $a^{-1}c, a^{-1}e \in \mathcal{D}$ exactly when the intersection has at least two elements.

Conversely, if $e \in F^*$ is such that $e = 1 - \lambda b$ for some $\lambda \in \Phi$, and that $|\Phi a \cap (\Phi c + e)| = \ell > 0$, then the equation $ax^m + by^m - cz^m = 1$ readily has ℓm^3 solutions from $(F^*)^3$.

Thus, the factor for m^3 is given by

$$\begin{aligned}\sum_{\lambda\in\Phi} |\Phi a \cap (\Phi c + (1 - \lambda b))| &= \sum_{\lambda\in\Phi} |(\Phi a + \lambda c) \cap (1 - \Phi b)| \\ &= |(\cup_{\lambda\in\Phi}(\Phi a + \lambda c)) \cap (1 - \Phi b)|.\end{aligned}$$

Some examples will illustrate what we put down above.

Our first example illustrates the general situation in which Algorithm 4 applies outside the circular setting. Here reduction succeeds and prime eligibility fails, so Algorithms 1–3 do not apply. This shows that Algorithm 4 functions in the noncircular case as well, providing the correct intersection counts and solution enumeration.

Example 6.3. Consider $F = \mathrm{GF}(41^2)$ with $k = 8$, so $m = 210$. Since $41 \in \mathcal{Q}_8$, for arbitrary $a, b, c \in F^*$, Algorithms 1–3 are not applicable. Let ζ be a primitive element, and $\Phi = \langle \zeta^{210} \rangle$. Let $a = \zeta^{420}$ and $b = c = \zeta^{1008}$.

(1) With $a \in \Phi$ and $b = c \notin \Phi$, $n_0 = m$.

(2) We have

$$\begin{aligned}\Phi \cap (\Phi a + b) &= \varnothing, \\ \Phi \cap (\Phi a - b) &= \varnothing, \\ \Phi \cap (\Phi b - b) &= \{\zeta^{420}, \zeta^{630}, \zeta^{1260}\},\end{aligned}$$

and so $t = 3$. Note that the third intersection shows that (F, Φ) is not circular.

(3) Next, since $a \in \Phi$, we have

$$\cup_{\lambda \in \Phi}(\Phi a + \lambda(-c)) = \cup_{\lambda \in \Phi}(\lambda a + \Phi(-c)) = \cup_{\lambda \in \Phi}(\lambda - \Phi b),$$

and so

$$1 - \Phi b \subseteq \cup_{\lambda \in \Phi}(\Phi a + \lambda(-c)).$$

This gives

$$|(1 - \Phi b) \cap (\cup_{\lambda \in \Phi} (\Phi a + \lambda(-c)))| = |1 - \Phi b| = k.$$

Hence the number of solutions of the equation $ax^m + by^m - bz^m = 1$ is

$$N = km^3 + 3m^2 + m = 8m^3 + 3m^2 + m = 74,220,510.$$

The next example highlights the complementary case. Whereas Example 6.3 shows reduction succeeds but prime eligibility fails, Example 6.4 demonstrates that when reduction itself fails, prime eligibility becomes irrelevant. Here we again take $F = \mathbb{Z}_{193}$ with $k = 8$, which gives a circular Ferrero pair, and Algorithm 4 may yield no solutions.

Example 6.4. Consider $F = \mathbb{Z}_{193}$ with $k = 8$ so $m = 24$. Take $\zeta = 5$. We have $F^* = \langle \zeta \rangle$, and $\Phi = \langle 9 \rangle = \{9, 81, 150, 192, 184, 112, 43, 1\}$. Note that (F, Φ) is circular. Let $a = \zeta = 5$, $b = \zeta^5 = 37$, and $c = \zeta^6 = 185$.

(1) As $a, b, c \notin \Phi$, we see that $ax^m = 1$, $by^m = 1$, and $cz^m = 1$ has no solutions in F.

(2) We have

$$\Phi a + b = \{42, 59, 18, 185, 32, 15, 56, 82\},$$
$$\Phi a - c = \{13, 30, 182, 156, 3, 179, 27, 53\},$$
$$\Phi b - c = \{45, 55, 99, 61, 164, 154, 110, 148\},$$

and all three have empty intersection with Φ. Thus, there is no solution for the equation $ax^m + by^m - cz^m = 1$ with $0 \in \{x, y, z\}$.

(3) Also one checks that $1 - \Phi b$ and $\cup_{\lambda \in \Phi}(\Phi a + \lambda(-c))$ are disjoint, and so there are no $\lambda_1, \lambda_2, \lambda_3 \in \Phi$ such that $a\lambda_1 + b\lambda_2 - c\lambda_3 = 1$.

Thus, $5x^m + 37y^m - 185z^m = 1$ has no solutions over $\mathbb{Z}_{193}$.

We continue with the same parameters $F = \mathbb{Z}_{193}$ and $k = 8$ as in Example 6.4, and provide with this circular Ferrero pair a setting in which Algorithm 4 distributes contributions among the m^3, m^2, and m terms.

Example 6.5. In this example, we consider $F = \mathbb{Z}_{193}$ with $k = 8$ and $\zeta = 5$.

Suppose that we take $a = 1$, $b = \zeta$, and $c = \zeta^4 = 46$. Then one checks that $1 - \Phi b$ and $\cup_{\lambda \in \Phi}(\Phi a + \lambda(-c))$ are disjoint, and so there are no $\lambda_1, \lambda_2, \lambda_3 \in \Phi$ such that $a\lambda_1 + b\lambda_2 - c\lambda_3 = 1$. The total number of solutions (with zero is involved) for the equation $ax^m + by^m - cz^m = 1$ is $m^2 + m = 600$.

If we take $a = \zeta = 5$, $b = \zeta^2$, and $c = \zeta^5$. As $a, b, c \notin \Phi$, we see that $ax^m = 1$, $by^m = 1$, and $cz^m = 1$ has no solutions in F. One checks that $\Phi a + b$, $\Phi b - c$, and $\Phi a - c$ all have empty intersection with Φ. Therefore, there are no solutions with zero is involved. Indeed, the number of solutions of $ax^m + by^m - cz^m = 1$ is $3m^3$.

Next are two more examples, taken from circular Ferrero pairs in a different finite field, which further illustrate the possible distributions of contributions among the m^3, m^2, and m terms.

Example 6.6. Let us consider the Galois field $F = \mathrm{GF}(19^2)$ with primitive element ζ. For $k = 10$, the equation $x^m + \zeta^{20}y^m - \zeta z^m = 1$, where $m = (19^2 - 1)/10 = 36$ and ζ^{20} is in the prime subfield of F, has $2m^3 + m^2 + m$ solutions. The m^3 part came from the solutions without zeros; the m^2 part came from the solutions with $z = 0$ but $x \neq 0$ and $y \neq 0$; the m part came from the solutions with $y = z = 0$.

On the other hand, the equation $x^m + \zeta^{100}y^m - \zeta z^m = 1$ has $4m^3 + m$ solutions. The m^3 part came from the solutions from $(F^*)^3$. Note that there are four λ's in Φ satisfying $|\Phi a \cap (\Phi c + (1 - b\lambda))| = 1$, each contributes m^3 solutions to the equation. Finally, the m part came from the solutions with $y = z = 0$.

Examples 6.4, 6.5, and 6.6 together demonstrate that in circular pairs, all possible combinations of contributions can occur: absence of the m^3 term, absence of the m^2 term, absence of the m term, as well as cases where all three appear simultaneously. This confirms that the three-stage decomposition of Algorithm 4 is exhaustive, and that each type of contribution is realized in practice.

References

[1] J. R. Clay. *Nearrings: Geneses and Applications*. Oxford University Press, Oxford, 1992.

[2] J. H. Conway and A. J. Jones. Trigonometric diophantine equations (On vanishing sums of roots of unity). *Acta Arithmetica*, 30(3):229–240, 1976.

[3] L. E. Dickson. Congruences involving only e-th powers. *Acta Arithmetica*, 1:161–167, 1936.

[4] O. B. Faircloth. On the number of solutions of some general types of equations in a finite field. *Canadian Journal of Mathematics*, 4:343–351, 1952. https://doi.org/10.4153/CJM-1952-030-0.

[5] L.-K. Hua and H. S. Vandiver. Characters over certain types of rings with applications to the theory of equations in a finite field. *Proceedings of the National Academy of Sciences of the United States of America*, 35(2):94–99, 1949. https://doi.org/10.1073/pnas.35.2.94.

[6] L.-K. Hua and H. S. Vandiver. On the number of solutions of some trinomial equations in a finite field. *Proceedings of the National Academy of Sciences of the United States of America*, 35(8):477–481, 1949. https://doi.org/10.1073/pnas.35.8.477.

[7] K. F. Ireland and M. I. Rosen. *A Classical Introduction to Modern Number Theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, Heidelberg, and New York, 2nd edition, 1990. https://doi.org/10.1007/978-1-4757-2103-4.

[8] J.-R. Joly. Équations et variétés algébriques sur un corps fini. *L'Enseignement Mathématique*, 19(2):1–117, 1973.

[9] W.-F. Ke and H. Kiechle. On the solutions of the equation $x^m + y^m - z^m = 1$ in a finite field. *Proceedings of the American Mathematical Society*, 123(5):1331–1339, 1995. https://doi.org/10.1090/S0002-9939-1995-1234628-4.

[10] W.-F. Ke and H. Kiechle. Combinatorial properties of ring generated circular planar nearrings. *Journal of Combinatorial Theory, Series A*, 73(2):286–301, 1996. https://doi.org/10.1006/jcta.1996.0023.

[11] W.-F. Ke and H. Kiechle. Overlaps in field generated circular planar nearrings. *Algebra and Discrete Mathematics*, 35(2):134–167, 2023. https://doi.org/10.12958/adm2130. arXiv: 2307.07303 [math.CO].

[12] W.-F. Ke and H. Kiechle. Circularity in finite fields and solutions of the equations $x^m + y^m - z^m = 1$. *Finite Fields and Their Applications*, 98:102467, 2024. https://doi.org/10.1016/j.ffa.2024.102467. arXiv: 2307.05586 [math.NT].

[13] H. Kiechle. Points on fermat curves over finite fields. In G. L. Mullen and P. J.-S. Shiu, editors, *Finite Fields: Theory, Applications, and Algorithms*. Volume 168, Contemporary Mathematics, pages 181–183. American Mathematical Society, Providence, RI, 1994.

[14] D. H. Lehmer. The number of solutions of a certain congruence involving the sum of like powers. *Utilitas Mathematica*, 39:65–89, 1991.

[15] M. C. Modisett. A characterization of the circularity of balanced incomplete block designs. *Utilitas Mathematica*, 35:83–94, 1989.

[16] T. Storer. *Cyclotomy and Difference Sets*, volume 2 of *Lectures in Advanced Mathematics*. Markham Publishing Co., Chicago, IL, 1967.

[17] The GAP Group. *GAP – Groups, Algorithms, and Programming*. Version 4.15.1. The GAP Group. 2025.

[18] The PARI Group. *User's Guide to PARI/GP*. Version 2.17.2. The PARI Group. 2025.

[19] A. Weil. Numbers of solutions of equations in finite fields. *Bulletin of the American Mathematical Society*, 55(5):497–508, 1949. https://doi.org/10.1090/S0002-9904-1949-09219-4.

[20] J. Wolfmann. The number of solutions of certain diagonal equations over finite fields. *Journal of Number Theory*, 42(3):247–257, 1992. https://doi.org/10.1016/0022-314X(92)90091-3.

Wen-Fong Ke
Department of Mathematics, National Cheng Kung University, Tainan, Taiwan
E-mail wfke@mail.ncku.edu.tw

Hubert Kiechle
Universität Hamburg, Fachbereich Mathematik, Bundesstr, 55, Hamburg, Germany
E-mail hubert.kiechle@uni-hamburg.de